



Microsoft IIS 6



What can you do with IIS?

MSTP

- Host an inter/intranet web site
- Provide FTP services
- Use Web and Public folders for collaboration
- Must be installed to use OWA
- Exchange uses it's SMTP Virtual Server
- Supports multiple mail protocols
- Local MMC or Remote Administration from a browser
- NNTP Services

IIS Supports TCP/IP Protocols



MSTP

- Hypertext Transfer Protocol--HTTP
- File Transfer Protocol--FTP
- Simple Mail Transfer Protocol--SMTP
- Network News Transfer Protocol--NNTP
- Post Office Protocol version 3--POP3
- Internet Messaging Access Protocol—IMAP4



Introducing IIS 6

MSTP

- Features in IIS 6
- Introduction to the Windows Server 2003 Family
 - Availability
- Server Roles
- Compatibility

Components and Executables for IIS



MSTP

Service	Primary DLL Component	Service Host
World Wide Publishing service (WWW service)	Iisw3adm.dll	Svchost.exe
File Transfer Protocol service (FTP service)	Ftpsvc2.dll	Inetinfo.exe
Simple Mail Transfer Protocol service (SMTP service)	Smtpsvc.dll	Inetinfo.exe
Network News Transfer Protocol service (NNTP service)	Nntpsvc.dll	Inetinfo.exe
IIS Admin service	Iisadmin.dll	Inetinfo.exe



Main Features of IIS 6

MSTP

Feature	Impact
Application Health Monitoring	Improves the monitoring capabilities available to administrators for Web applications.
New Request Processor	Separates the IIS server component from the underlying OS and supporting applications, creating a more stable and secure platform that's less vulnerable to request-based attacks.
Dynamic Content Caching	Enables content generated dynamically, which essentially doesn't change, to be cached by IIS for improved performance and lower CPU overhead.
ASP Template Caching	ASP templates are now stored on disk after processing from the ASP file, eliminating the need to recompile ASP templates that have expired from the in-memory cache.
Process Isolation	Enables the administrator to assign different applications to different execution pools; if an application fails or ties up the pool, other application pools continue to operate.
ExecuteURL	Enables ISAPI filters to redirect requests to an alternative URL for processing.
Passport Integration	Enables Single Sign On (SSO) facilities for users with a valid Passport.
Low Privilege Execution	IIS now runs under a user with exceptionally low privileges, eliminating another potential weak point in security.
Lockdown mode	Shuts off all but the most basic static content—with dynamic content having to be specifically and individually enabled, which further reduces potential weak points.
XML Metabase	Enables for the easy modification and sharing of the configuration information stored in the metabase just by editing or copying the XML.
.NET Framework	Provides integration with the .NET system, including technologies such as Passport and dynamic systems, as well as languages supported by the .NET environment.
Improved Logging	IIS 6 can now log using UTF-8 (Unicode) text, useful for foreign language Web sites. A new binary mode makes for a more efficient and performance friendly method of logging compared to the text-based W3C format.
Granular Compression	Compression for responses can now be set at a more granular level, enabling compression on individual Web sites or folders instead of the whole server.

Windows Server 2003 Family



MSTP

- Windows Server 2003, Standard Edition
 - limit of 4 CPUs, 4GB of RAM, and 4TB of disk space, it's unsuitable for higher-demand IIS applications.
 - Standard Edition is also limited only to Network Load Balancing in multiserver environments
 - Web Edition will probably offer a more cost effective solution.

Windows Server 2003

Cont.



MSTP

- Windows Server 2003, Enterprise Edition
 - Up to eight-way CPU systems can be used with Enterprise Edition, and it's the first version to support the 64-bit Itanium processor when it becomes available.
 - maximum RAM capability to 32GB
 - supports Address Windows Extensions (AWE), which in a 4GB server can specifically reserve just 1GB for the core operating system, enabling the remaining 3GB to be used by applications

In the Standard and Web Editions, the addressable memory is split equally between the OS and applications.

Windows Server 2003 Cont.



MSTP

- Windows Server 2003, Datacenter Edition
 - Datacenter Edition is only available with the very high-end, top of the range and limits of current technology type hardware that you can normally only dream of
 - support for up to 64GB of RAM (256GB on Itanium) and 32 processors (64 on Itanium).
 - Clustering support remains the same at 8 nodes per cluster.

Windows Server 2003

Cont.



MSTP

- Windows Server 2003, Web Edition
 - limited to two processors and just 2GB of RAM.
 - units are 'pizza box' style
 - 1U high stacked into numerous 19 inch rack mount cupboards
 - large rack will take 42 1U high units: That's 42 dual-processor machines—all of which could be part of an NLB structure for handling thousands of Web site requests every second.
 - Web Edition also removes the need for the usual licensing restrictions



Server Roles

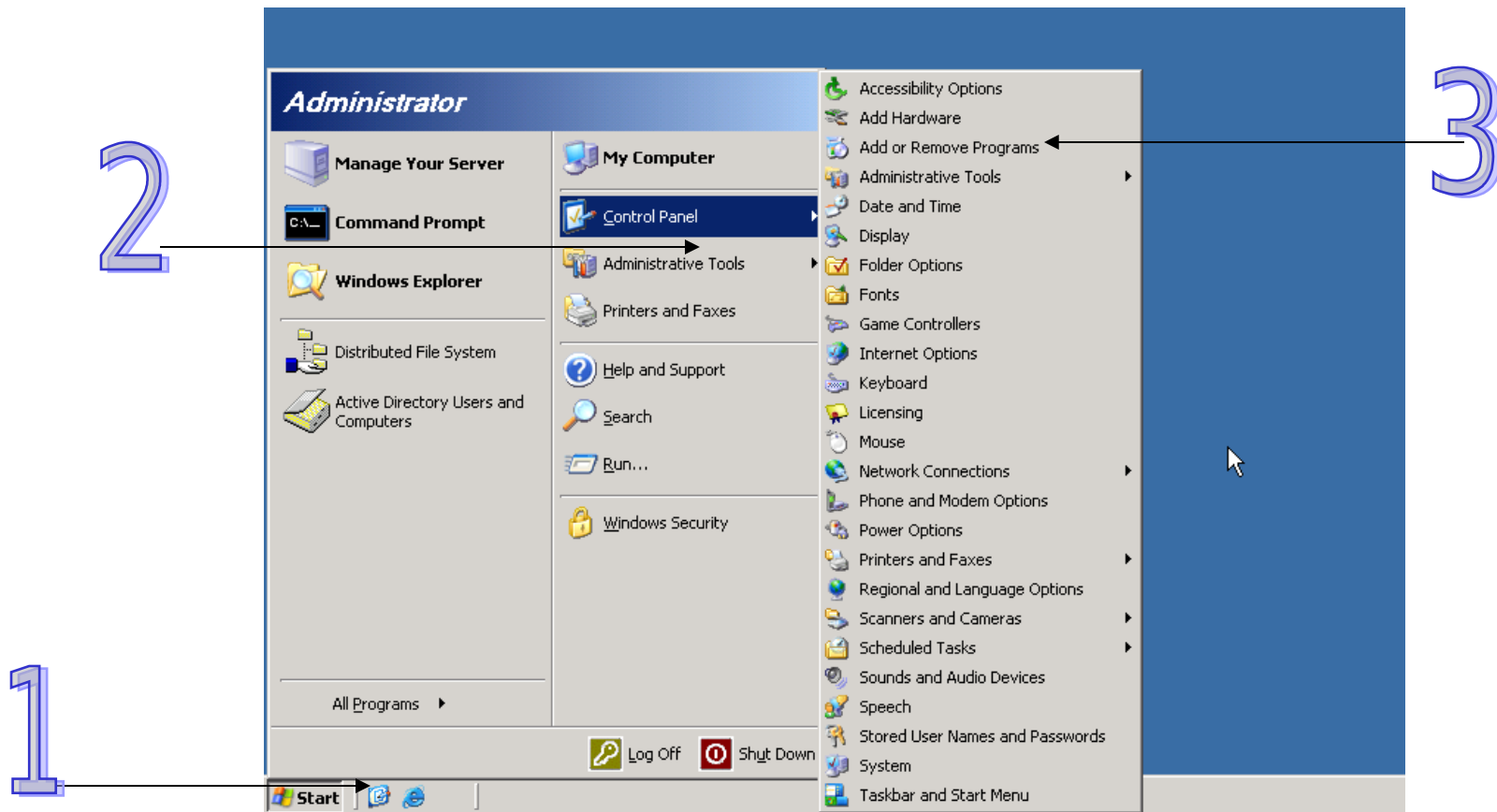
MSTP

- key technologies installed by selecting the Application Server role are
 - Internet Information Server
 - ASP
 - ASP.NET
 - COM+
 - Microsoft Message Queuing (MSMQ)



Installing IIS

MSTP





Installing IIS Cont..

MSTP

1 Click Here

2 Click Here

3 Click Here

4

5 Click Here

Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

Component	Size
<input type="checkbox"/> Application Server Console	0.0 MB
<input checked="" type="checkbox"/> ASP.NET	0.0 MB
<input checked="" type="checkbox"/> Enable network COM+ access	0.0 MB
<input type="checkbox"/> Enable network DTC access	0.0 MB
<input checked="" type="checkbox"/> Internet Information Services (IIS)	18.1 MB
<input type="checkbox"/> Message Queuing	6.5 MB

Description: IIS includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 4.2 MB
Space available on disk: 4696.0 MB

Details... OK Cancel

< Back Next > Cancel Help



Wizard Installation Method

MSTP

Manage Your Server
Server: BESTPRAC

Search Help and Support Center

Managing Your Server Roles

Use the tools and information found here to add or remove roles and perform your daily administrative tasks.

Your server has been configured with the following roles:

- File Server**
 - File servers provide and manage access to files.
 - [Add or remove a role](#)
 - [Read about server roles](#)
 - [Read about remote administration](#)
- Application Server**
 - Application servers provide the core technologies required to build, deploy and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+, and Internet Information Services (IIS).
 - [Manage this file server](#)
 - [Add shared folders](#)
 - [Review the next steps for this role](#)
 - [Read about application servers](#)
 - [Read about Web Interface for Remote Administration of Web servers](#)
 - [Review the next steps for this role](#)
- Domain Controller (Active Directory)**
 - Domain controllers use Active Directory to manage network resources such as users, computers, and applications.
 - [Manage users and computers in Active Directory](#)

Tools and Updates

- Administrative Tools
- More Tools
- Windows Update
- Computer and Domain Name Information
- Internet Explorer Enhanced Security Configuration

See Also

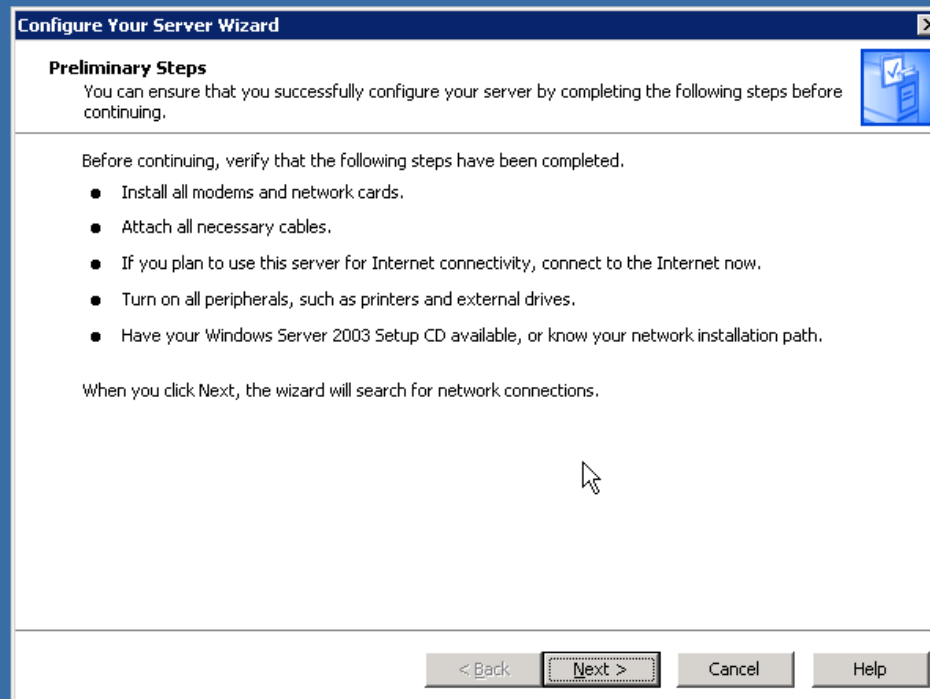
- Help and Support
- Microsoft TechNet
- Deployment and Resource Kits
- List of Common Administrative Tasks
- Windows Server Communities
- What's New
- Strategic Technology Protection Program

Double Click Here



Wizard Installation Method

MSTP





Wizard Installation Method

MSTP

Configure Your Server Wizard

Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open [Add or Remove Programs](#).

Server Role	Configured
File server	Yes
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	Yes
Remote access / VPN server	No
Domain Controller (Active Directory)	No
DNS server	Yes
DHCP server	Yes
Streaming media server	No
WINS server	No

Application server (IIS, ASP.NET)

Application servers provide the core technologies required to build, deploy, and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+ and Internet Information Services (IIS).

[Read about application servers](#)

< Back **Next >** Cancel Help



Wizard Installation Method

MSTP

Configure Your Server Wizard

Application Server Options
IIS, COM+, ASP.NET, and Microsoft .NET Framework are installed automatically for this role.

Select the additional tools that you want to install on this server.

☐ **FrontPage Server Extensions**
FrontPage Server Extensions are a set of Web server extensions that you can use to publish content with FrontPage, Visual Studio, and Web Folders.

☐ **Enable ASP.NET**
ASP.NET is a powerful programming framework for building Web-based applications and services that can target any browser or device.

< Back **Next >** Cancel Help



Wizard Installation Method

MSTP

Configure Your Server Wizard [X]

Summary of Selections
View and confirm the options you have selected.

Summary:

Install Internet Information Services (IIS)
Enable COM+ for remote transactions
Enable Microsoft Distributed Transaction Coordinator (DTC) for remote access

To change your selections, click Back. To continue setting up this role, click Next.

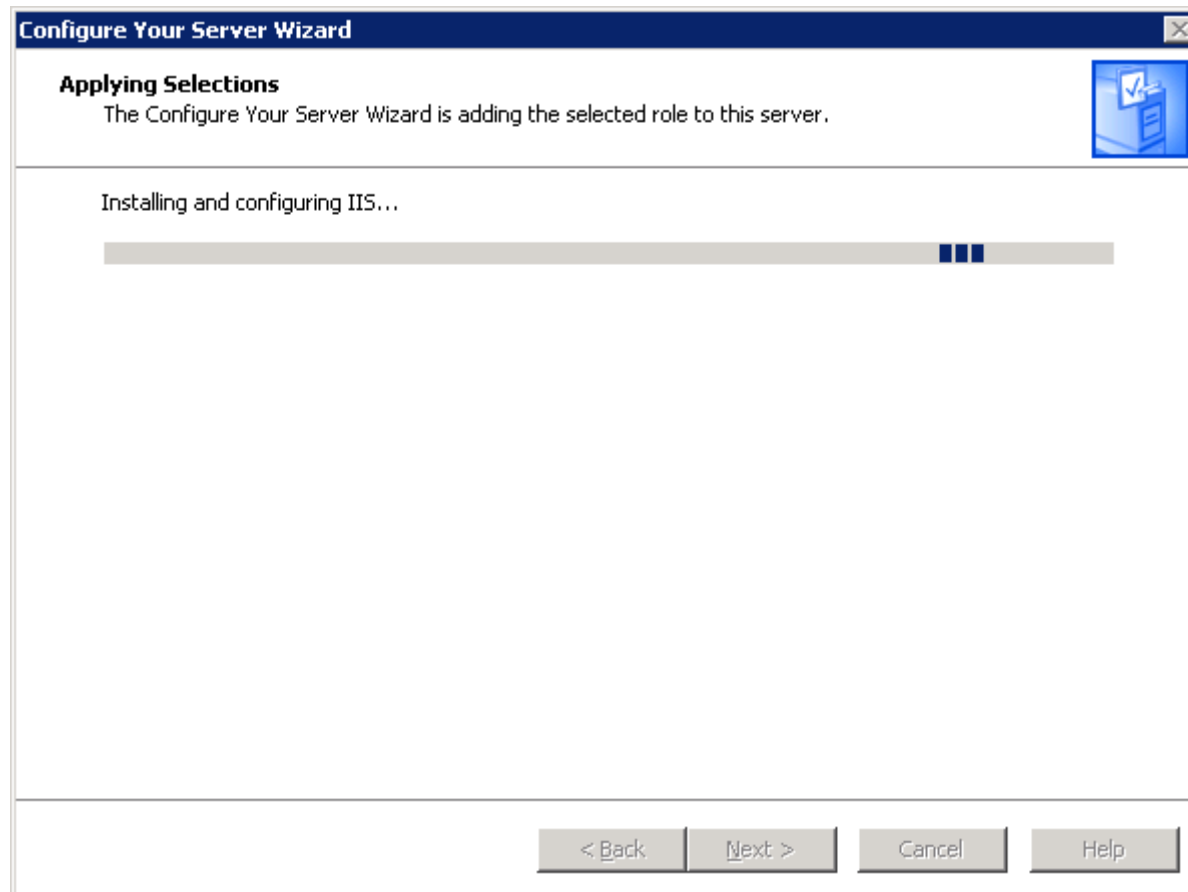
< Back **Next >** Cancel Help



Wizard Installation Method



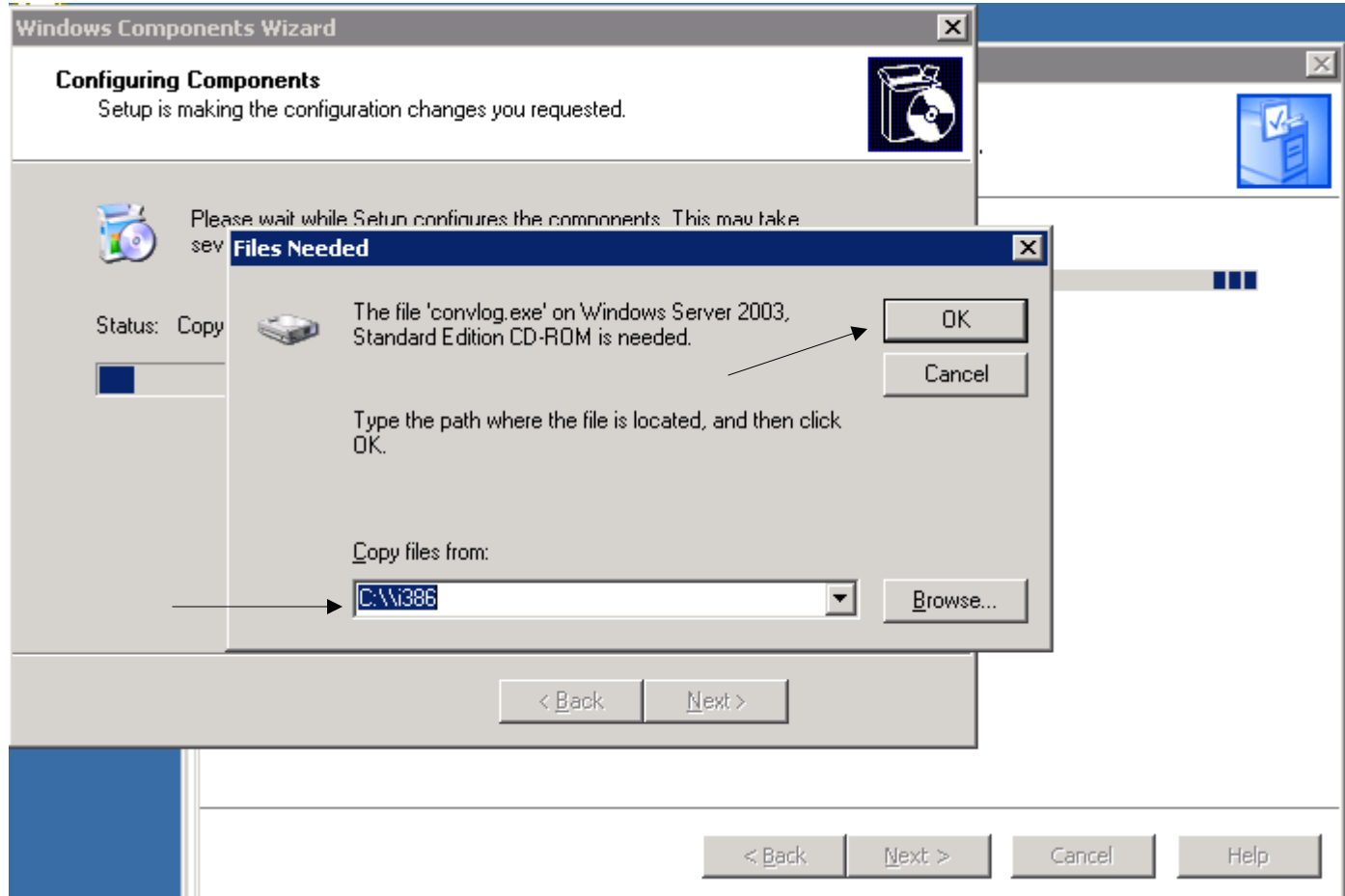
MSTP





Wizard Installation Method

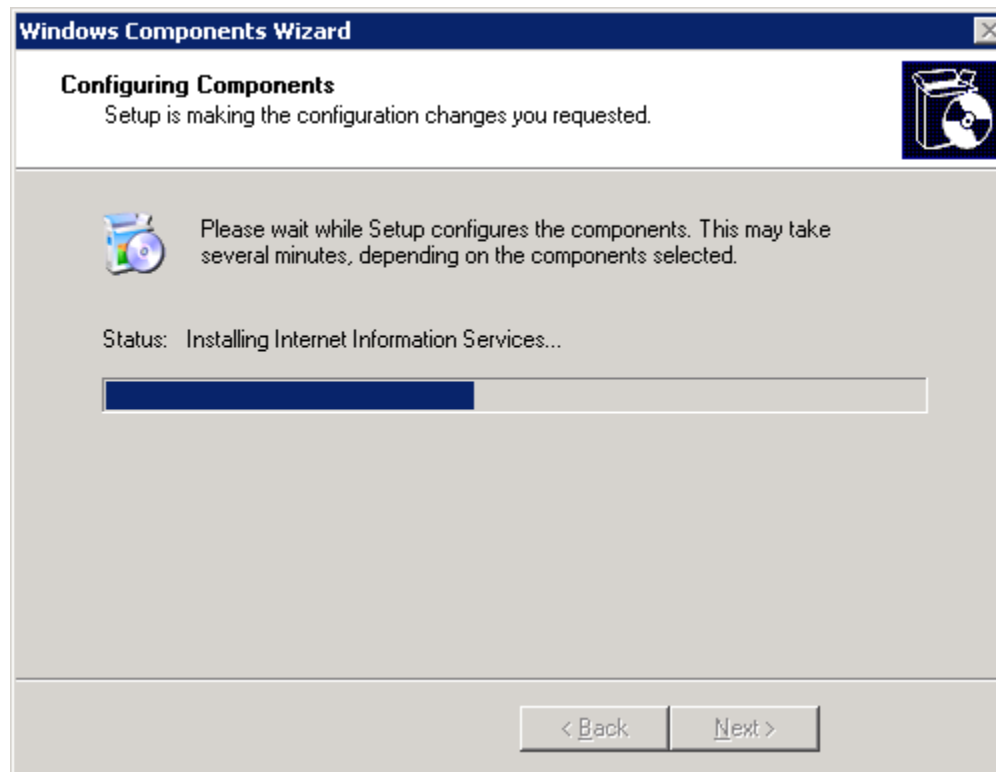
MSTP





Wizard Installation Method

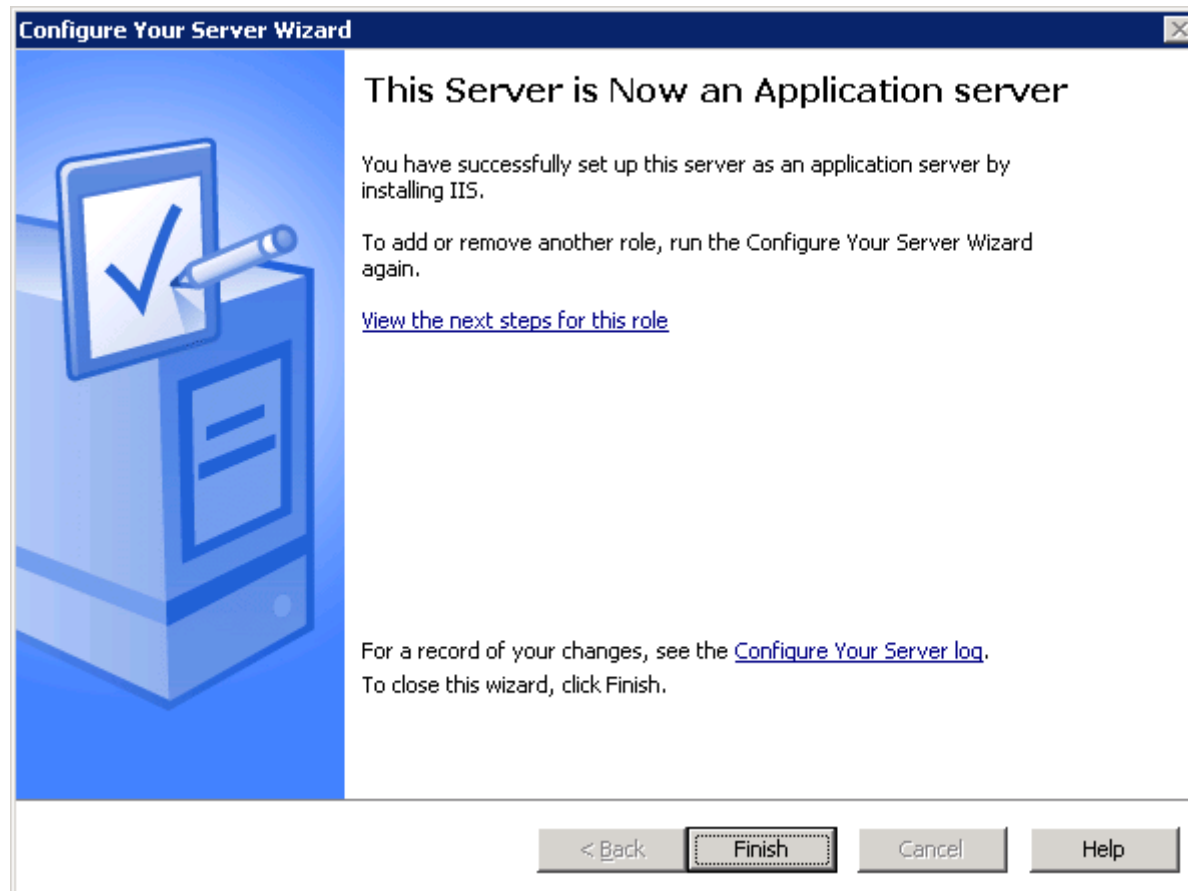
MSTP





Wizard Installation Method

MSTP





Compatibility

MSTP

- IIS 6 is still just a platform for serving Web pages
- IIS 6 will still provide static pages to clients who ask for them, and many other core features—such as the support for CGI and scripting technologies, ASP, FrontPage extensions, and so on—remain the same.
- IIS 6 work in a 100% compatible way with IIS 5, and anything that runs currently within IIS 5 should work identically when IIS 6 is operating in this mode.
- IIS 6 also includes a brand new Web-based interface for administration purposes, enabling you to monitor and manage your IIS installation even when MMC is not available.
- Compatibility with most third-party filters, languages, and support tools is also retained
 - IIS 6 is also the first IIS revision that closely matches the execution model of Apache.



Architecture and Execution

MSTP

- Understanding the new IIS 6 Architecture
- Configuring IIS 6 architecture parameters
- Working in IIS 5 Isolation Mode Configuration

Architecture



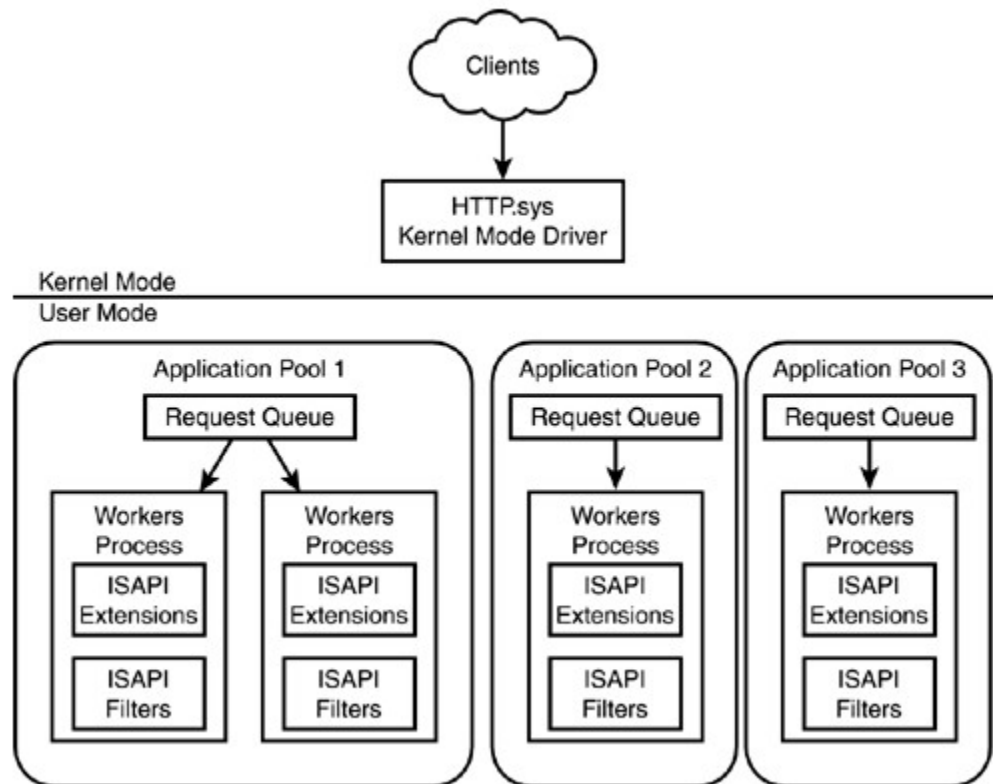
MSTP

- **Stability**— If an application supported through IIS crashes, the chances are that either it will crash IIS or it will 'steal' resources from other Web sites and applications.
- **Security**— If the application provides a method for accessing the application in a nondocumented fashion, you have a potentially lethal security breach that could be used to access your entire network.
- **Performance**— One top-heavy process has to deal the majority of the processing because a rogue user-mode application could be sapping CPU and memory from the other requests. Performance can be significantly impaired.
- **Scalability**— Because a single process is responsible both for accepting and processing many of the requests, clients can be waiting to communicate a request while another user is still being serviced. When scaling up to multiple processors or machines, the same basic bottleneck remains.
- **Integration**— Although previous versions gave the impression of being integrated into the OS, the reality is that IIS was just another application. If you're looking at the OS, Internet Service Manager and don't see any differences between IIS 5 and 6, it's because a lot is under the hood. This business of the kernel mode driver is a massive overhaul, and it truly makes IIS a part of the Windows OS now.



Worker Process Isolation Mode

MSTP





Worker Process Cont.

MSTP

- **Application Pools**

- Clean separation between the user and kernel code
- Multiple application pools
- Worker process management
- Rapid-fail protection
- Load balancing support

- **Request Queues**

- The request queue handles the incoming requests supplied by HTTP.sys waiting to be processed by the corresponding application pool.

Worker Processes

- Health monitoring;
- Processor affinity
- CPU monitoring
- Demand start
- Idle timeout
- Orphan control
- Manual recycling
- Automatic recycling (restarting)
 - Elapsed time
 - Number of requests served
 - Scheduled time within a 24-hour period
 - Result of a 'liveliness ping'
 - Virtual Memory usage
 - Physical Memory usage

WEB GARDENS

- multiple worker processes within a single application pool, IIS 6²⁷ operates as a Web garden.



- The WSAMC component handles two main areas configuration & process management.
 - responsible for distributing requests
 - managing the individual worker processes, including starting, stopping, and recycling processes



Web Application Isolation

MSTP

- The idea of Worker Process Isolation mode is to isolate user-mode operations into one or more application pools and in turn, one or more worker processes—all completely separate and also separate from the primary contact point, HTTP.sys.

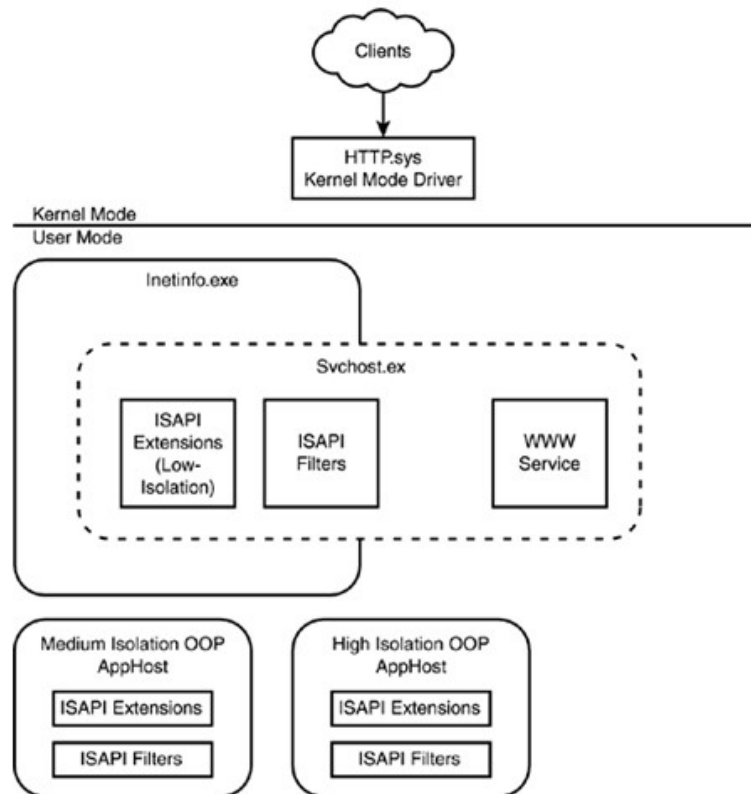


IIS 5 Isolation Mode

MSTP

IIS 5 Isolation Mode was designed to retain compatibility with applications that are currently being supported under IIS on Windows 2000.

The request model in IIS 5 Isolation Mode.





Web Application Isolation

MSTP

- Low (IIS Process)
- Medium (Pooled)
- High (Isolated)



Isolation Mode Comparison

MSTP

Comparing IIS 5 and Worker Process Isolation Modes

IIS Function	IIS 5 Isolation Mode		Worker Process Isolation Mode	
	Component	Application	Component	Application
Worker processes	N/A	N/A	WWW Service	Svchost.exe
Worker process management	N/A	N/A	Worker process	W3wp.exe
In-process ISAPI extensions		Inetinfo.exe	Worker process	W3wp.exe
Out-of-process ISAPI extensions		DLLHost.exe	(none)	(none)
ISAPI Filters		Inetinfo.exe	Worker process	W3wp.exe
HTTP.sys Config	WWW Service	Svchost.exe	WWW Service	Svchost.exe
HTTP Protocol	Windows kernel	HTTP.sys	Windows kernel	HTTP.sys
IIS Metabase		Inetinfo.exe		Inetinfo.exe
Authentication		Isass.exe	Worker process	W3wp.exe/Isass.exe
SSL		Inetinfo.exe		Isass.exe
FTP		Inetinfo.exe		Inetinfo.exe
NNTP		Inetinfo.exe		Inetinfo.exe
SMTP		Inetinfo.exe		Inetinfo.exe



Default Settings

MSTP

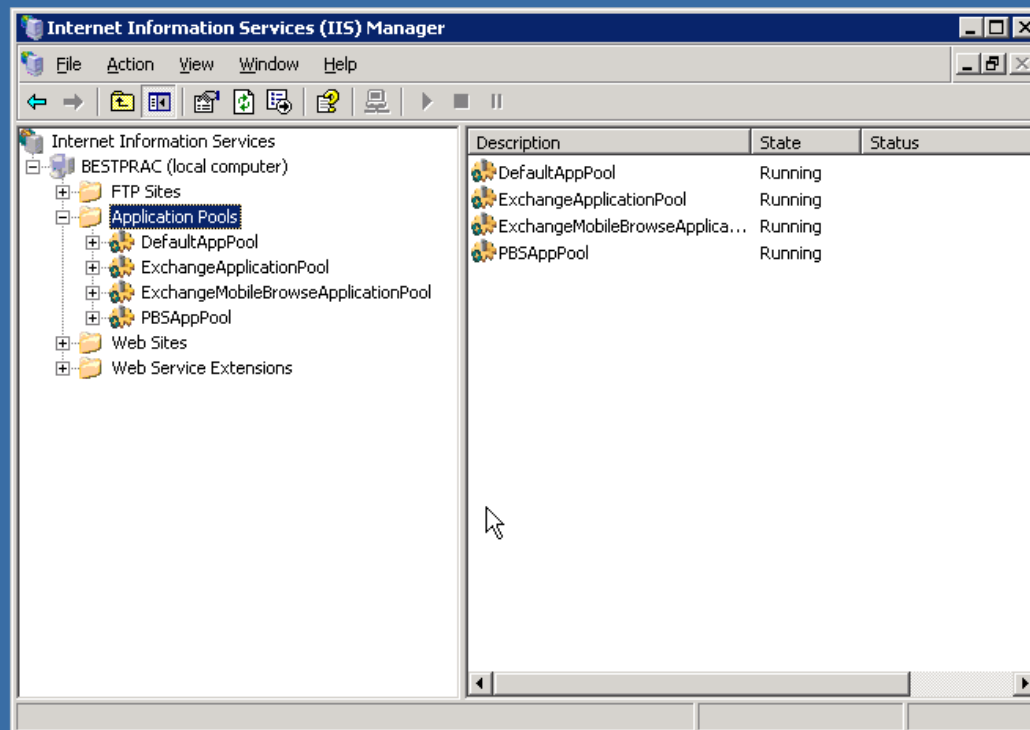
Default Operating Modes for Different Installation Types

Installation	Default Isolation Mode
New Installation	Worker process isolation mode
Upgrade from previous IIS 6 version	No change from previous mode
Upgrade from Windows 2000/IIS 5	IIS 5 Isolation Mode
Upgrade from Windows NT/IIS 4	IIS 5 Isolation Mode



AP-Configuration

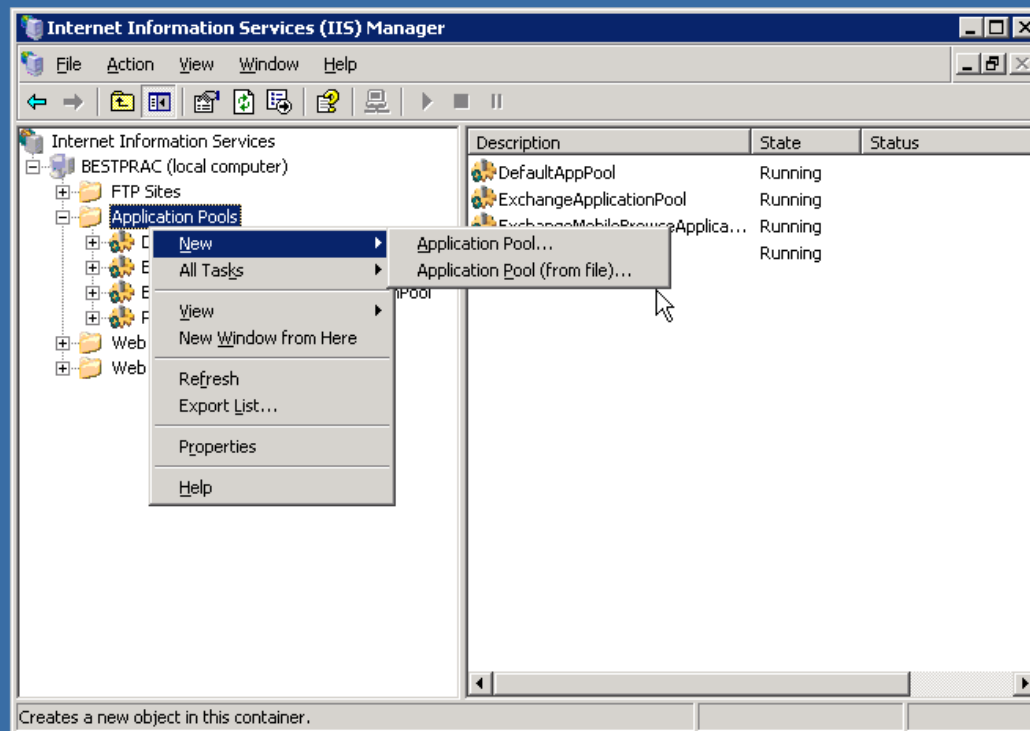
MSTP



Creating and Naming Application Pools



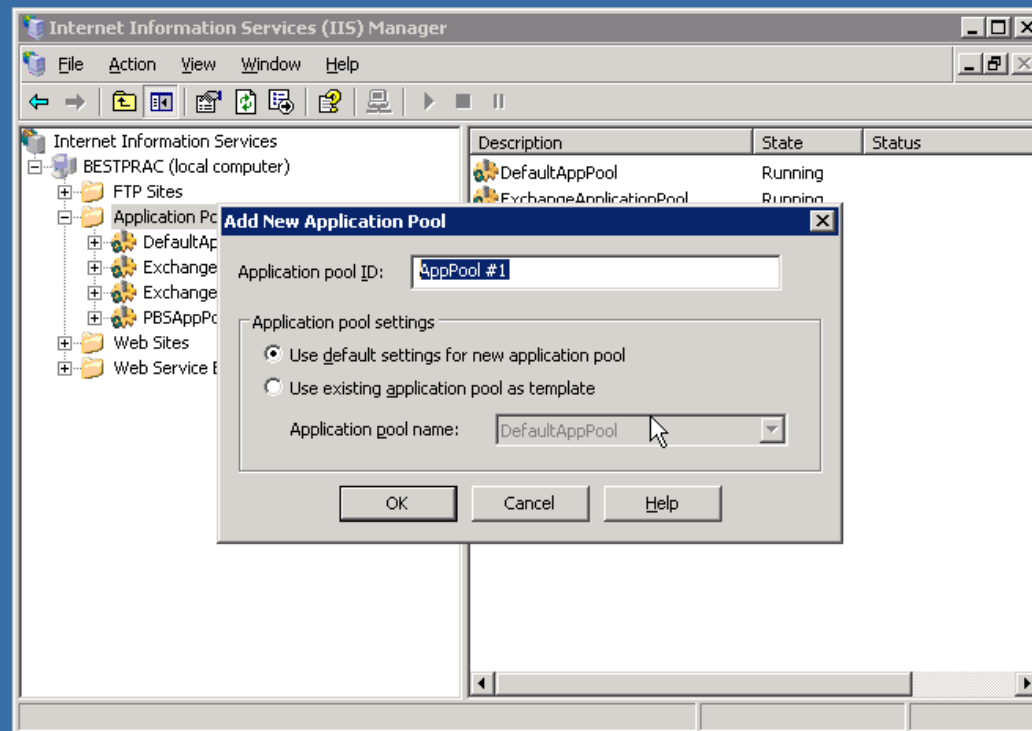
MSTP



Creating and Naming Application Pools

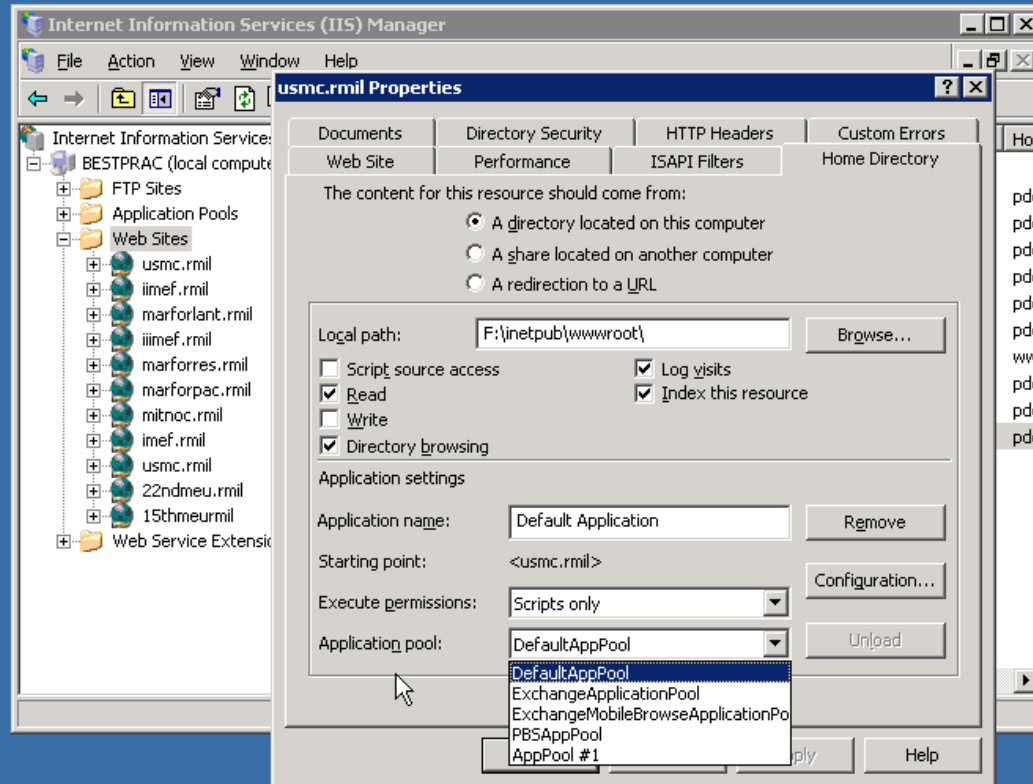


MSTP



Allocating Sites to Pools

MSTP





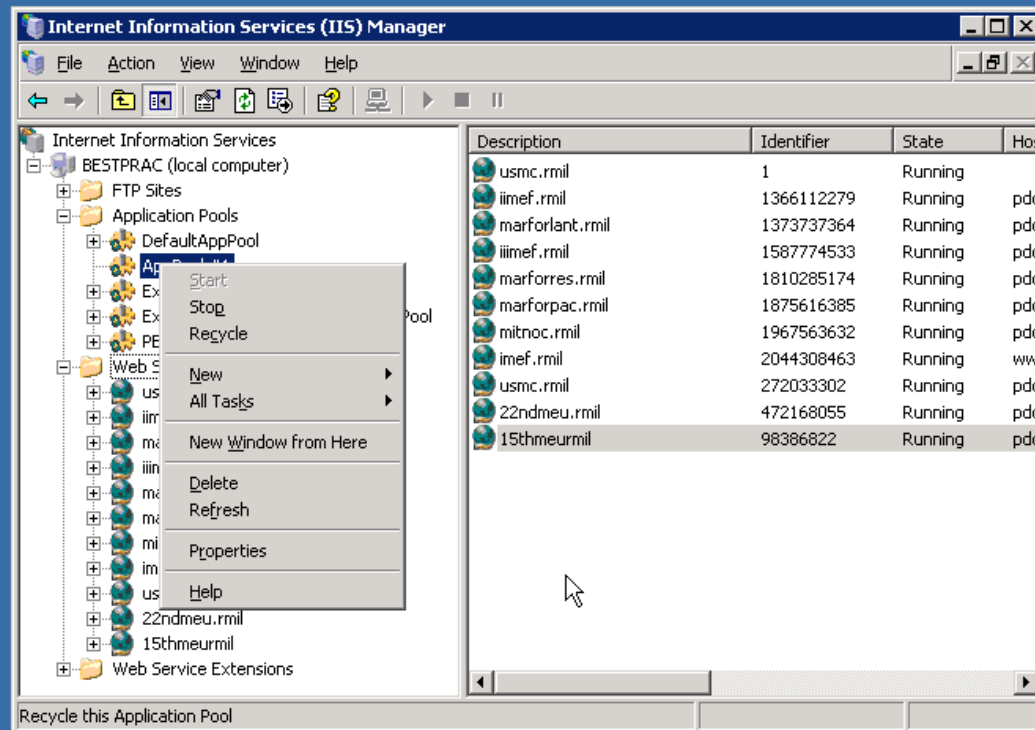
Starting and Stopping Pools

- Start
 - will start a currently stopped pool.
- Stop
 - will stop a currently running pool, enabling all applications that use this pool.
- Recycle
 - will shut down and then restart all the worker processes within the pool.
- Request Queue Parameters

Starting and Stopping Pools



MSTP



Sample Settings for the Request Queue Length



MSTP

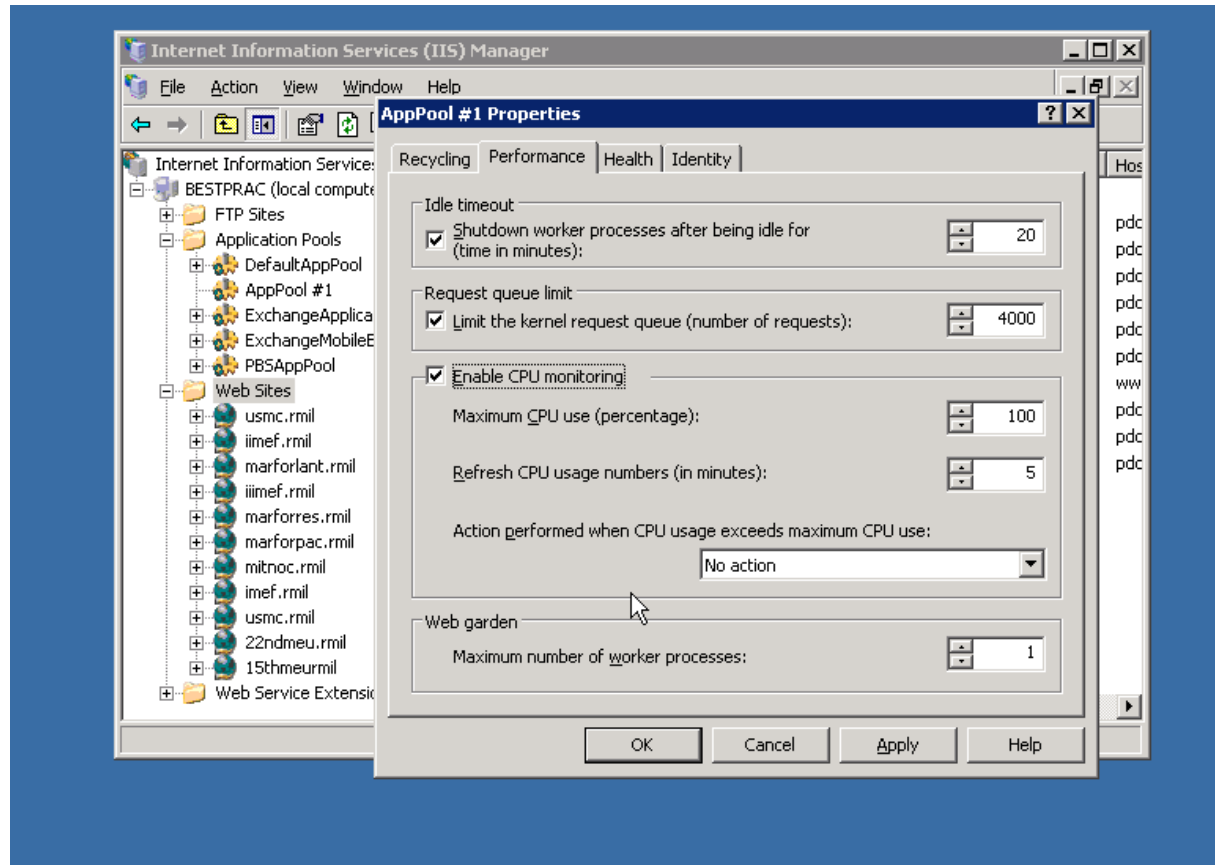
Sample Settings for the Request Queue Length

Site Type	Queue Setting	Discussion
Static Pages	1000-2000	With static pages, the server is really only reading a file off the disk and sending the data back to the client. This is a relatively light duty, so it takes little time to process. On a fast server, particularly one with two or more CPUs and employing multiple worker processes, you might be able to increase the values still further.
Built-in/Embedded ISAPI Filters	500-1000	These have a slightly larger load because additional code and applications will be required to process the requests. The ideal setting is highly application specific.
ASP/ASP.NET	250-500	ASP/ASP.NET implies a relatively high CPU requirement over static page provision, and therefore the value reflects this increased processing time. For simple applications, especially when using ASP for templating with the template caching option enabled, you could increase this to a value similar to that of the static pages. For solutions that process Web requests or provide interfaces to databases, keep in mind that the request time must include the time to process the DB request, as well as process the data and return the desired HTML.
CGI-based applications	125-250	Most CGI applications require the loading of an external process for the request to be processed. Starting a new application is one of the most intensive operations and so the load is significantly higher than an ISAPI based process.



Performance Parameters

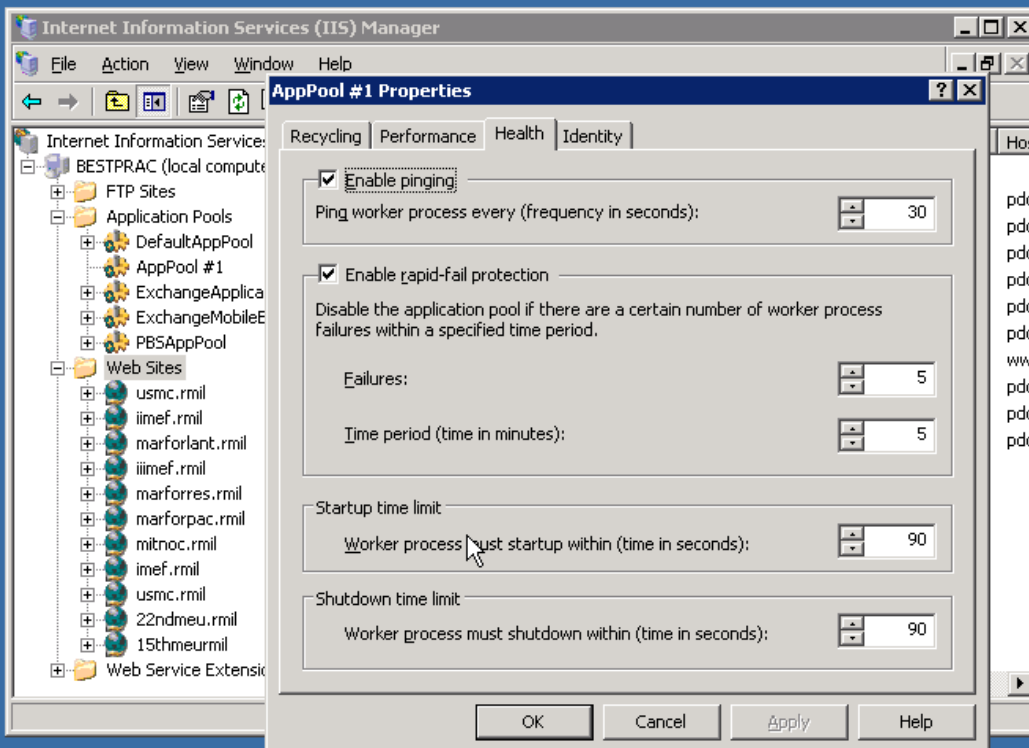
MSTP



Health Monitoring Parameters



MSTP





Switching to IIS 5 Isolation Mode

MSTP

If you want to change your server to run Web sites using IIS 5 Isolation Mode, implement the following steps:

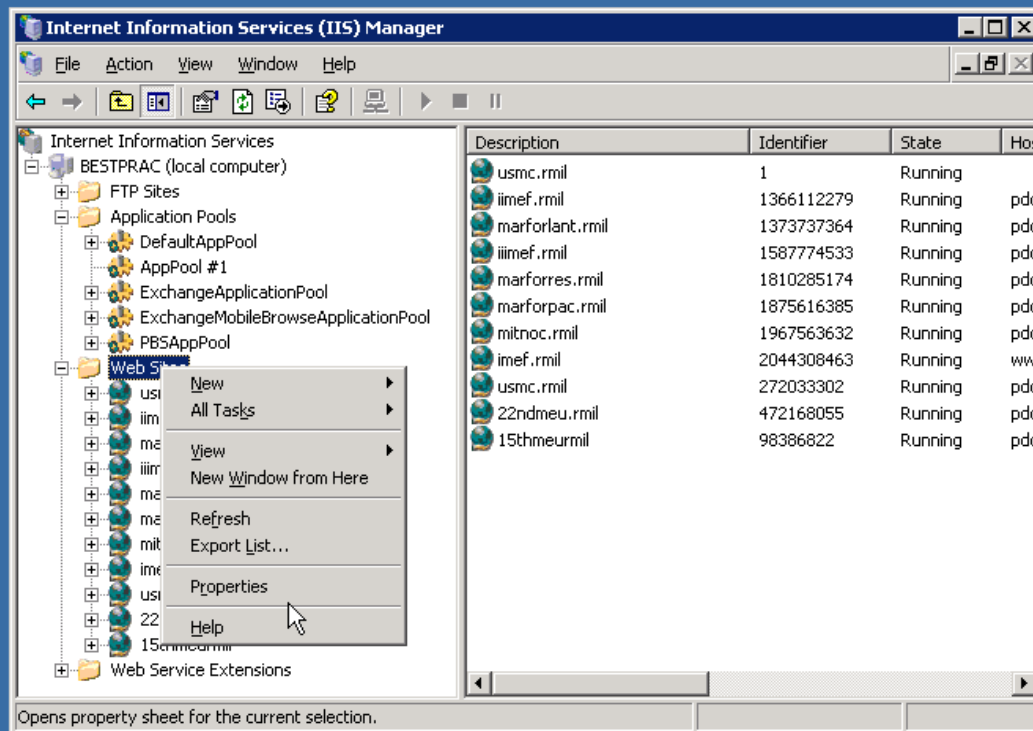
1. Open the Properties dialog box for all Web Sites within your server.
2. Click the Service tab.
3. Select Run WWW Service in IIS 5.0 Isolation Mode.
4. Click OK.
5. You will be prompted to accept the change. Click Yes to continue.

ISOLATION MODE DISABLES WORKER PROCESSES!

This will disable worker process isolation mode because the two modes cannot co-exist. Any existing requests will be completed before the change takes place; although it won't interrupt existing requests, new requests might have to wait until the existing requests have completed successfully.

Switching to IIS 5 Isolation Mode

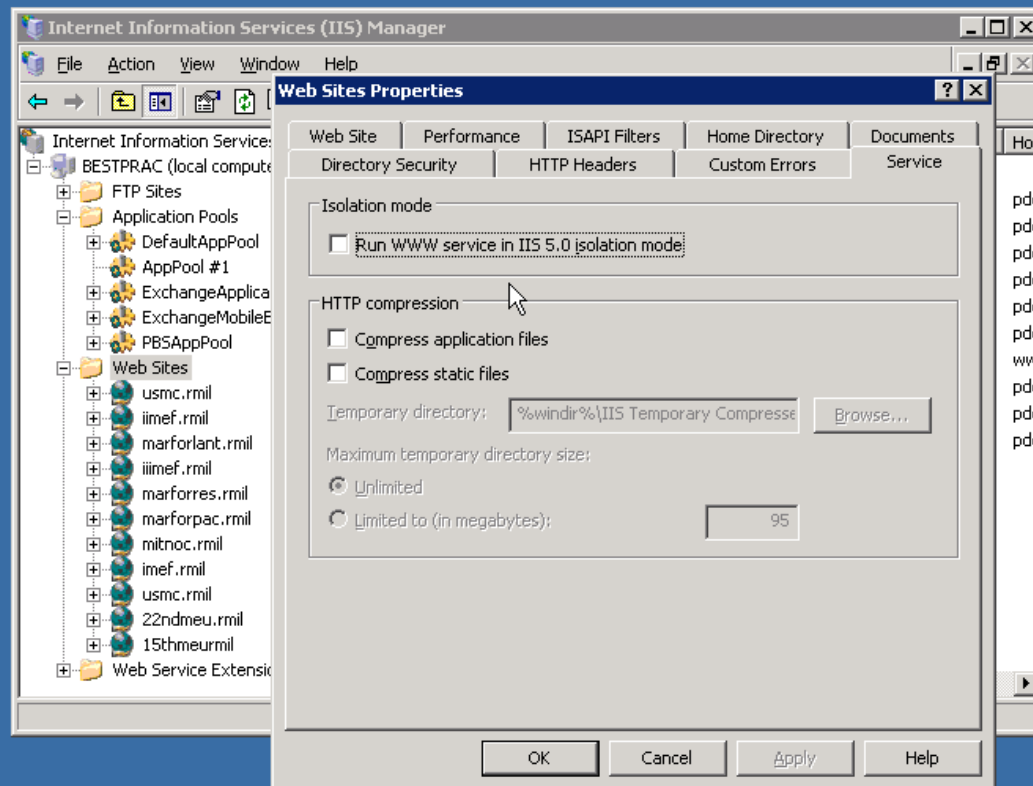
MSTP





Switching to IIS 5 Isolation Mode

MSTP



Start of Security



MSTP

- Unlocking the IIS 6 Server
- Passport.NET Authentication
- Setting the identity of Worker Processes

Locking/Unlocking a Server



MSTP

- There are three main steps between the unavailability of IIS when Windows Server 2003 is first installed to a running, functional, but still secure state:
 - Installing IIS (including upgrading from IIS 4/5)
 - Unlocking Static Content
 - Unlocking Web Services Extensions



Upgrading from IIS 4/5 (NT/W2K)

MSTP

- Windows Server 2003 should automatically pick up any of the sites you've configured on these machines and server just as if you'd set them up on a new machine.
- Windows Server 2003 disables the service if you upgrade a machine from either of these two platforms, if IIS have not been modified.



Unlocking Static Content

MSTP

- Once IIS has been installed and enabled through the Server Roles Wizard, it's still more secure than a base IIS 4 or 5 installation. In its default state, IIS is only capable of serving static Web pages. All dynamic content, including CGI and ASP based content, is not enabled.
- Static content is therefore unlocked as soon as you install IIS.

UNLOCK AT YOUR OWN RISK



MSTP

- Don't unlock any IIS functionality that you don't absolutely need.
- Leaving IIS locked down will help make it as secure and safe as possible.



Recognized File Extensions

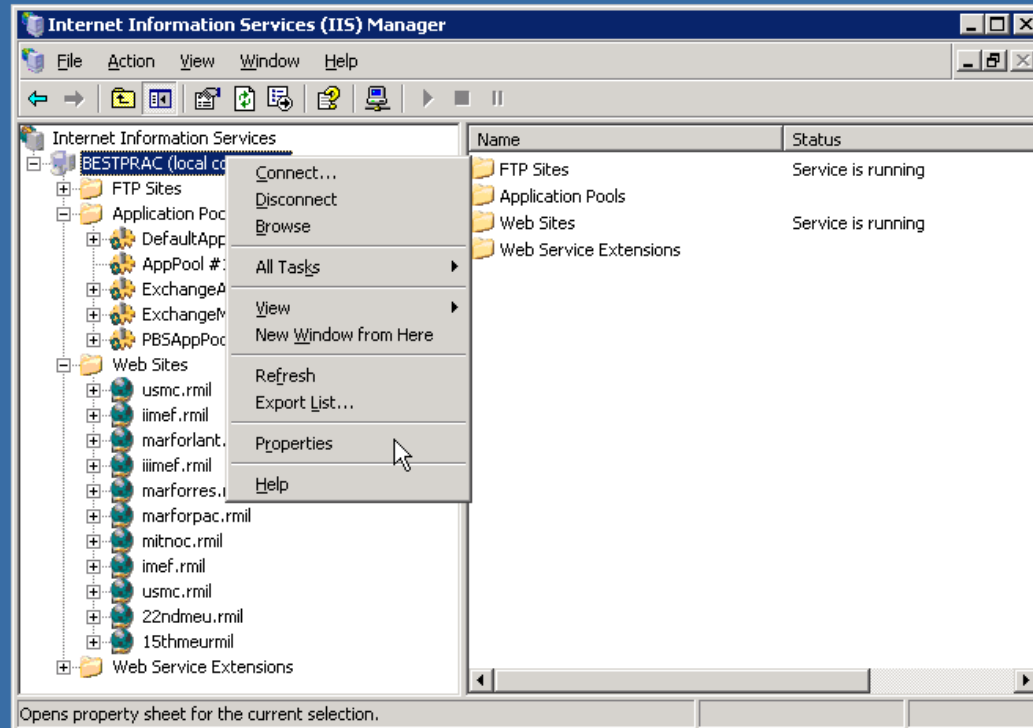
MSTP

- In addition to only serving static Web content, IIS also extends its restrictions on what it serves from a site.
- IIS 6 will only accept requests for files with extensions that it recognizes.
- You can manage the accepted MIME types that IIS will serve in two different places—at a server level and a Web site/directory level.

Default MIME types configured in IIS



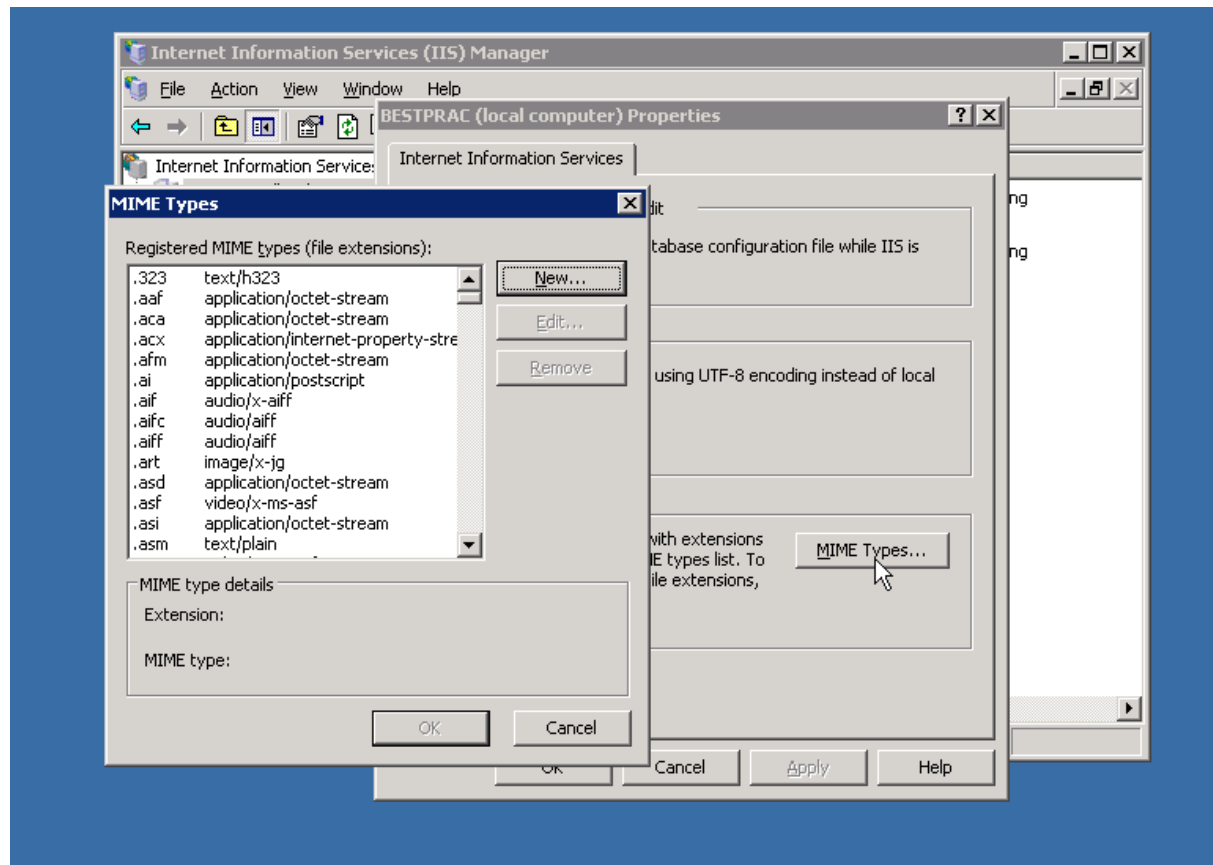
MSTP



Default MIME types configured in IIS



MSTP





Protected Web Content

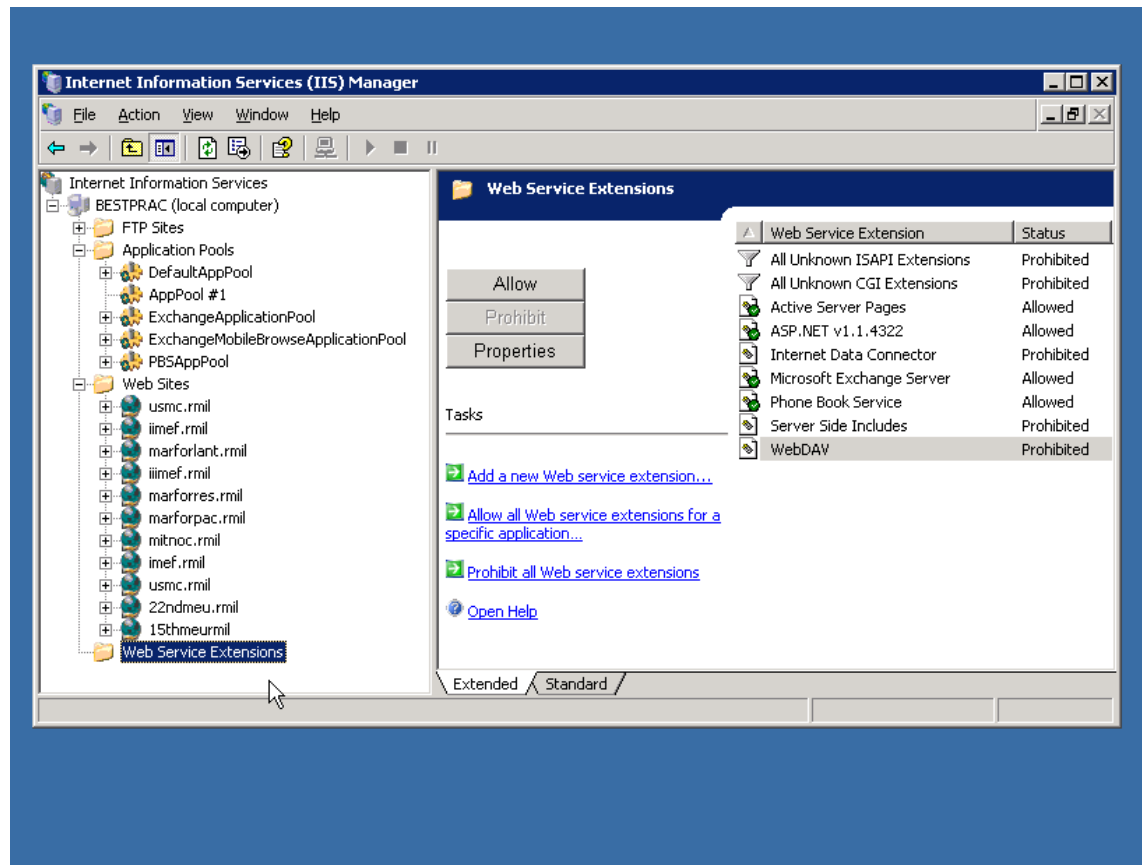
MSTP

- Most malicious attempts to access and use your IIS server rely on the ability to write files and to update and overwrite configuration files and others through the IIS service.
 - Within IIS 6, anonymous Web users are blocked from writing to the server.

The Web Services Extensions Manager



MSTP



Default Web Service Extension Security Settings



MSTP

Default Web Service Extension Security Settings

Web Service Extension	Notes
All Unknown ISAPI Extensions	You should leave this set to prohibited. Allowing unknown ISAPI extensions will make your system more susceptible to worm and virus attacks, such as the NIMDA/Code Red.
All Unknown CGI Extensions	You should leave this to prohibited and then only allow CGI extensions that you have specifically allowed.
Active Server Pages	Used to support the old ASP standard.
ASP.NET	Used to support the new ASP.NET standard and pages developed within the .NET Framework.
FrontPage Server Extensions	Used to support FrontPage extensions. You must enable this if you want users to administer and publish Web sites from a client computer, especially through tools such as FrontPage.
Internet Data Connector	Used to support simpler dynamic Web pages that display data from a database. If you are using ASP for your dynamic sites, you can usually leave this as prohibited.
Server Side Includes (SSI)	Used to support the SSI system and best left prohibited unless you specifically need the SSI system. If you are using ASP and SSI together, consider moving your templates entirely to ASP and disabling SSI support.
WebDAV	Used for the Web Distributed Authoring and Versioning System, which can be used to allow authenticated users to publish, lock, and manage files and resources on a Web site. WebDAV is generally more practical than FrontPage, but it's also a more open security risk if not properly managed, so make sure that it's prohibited unless required.



Adding a New Web Service Extension

MSTP

The screenshot shows the Internet Information Services (IIS) Manager console. The left pane displays the tree view with 'Web Service Extensions' selected. The right pane shows the 'Web Service Extensions' task area. A context menu is open over the 'Web Service Extensions' folder in the left pane, with the option 'Add a new Web service extension...' highlighted.

Web Service Extensions

Web Service Extension	Status
All Unknown ISAPI Extensions	Prohibited
All Unknown CGI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v1.1.4322	Allowed
Internet Data Connector	Prohibited
Microsoft Exchange Server	Allowed
Phone Book Service	Allowed
Server Side Includes	Prohibited
WebDAV	Prohibited

Tasks

- [Add a new Web service extension...](#)
- [Allow all Web service extensions for a specific application...](#)
- [Prohibit all Web service extensions](#)
- [Open Help](#)

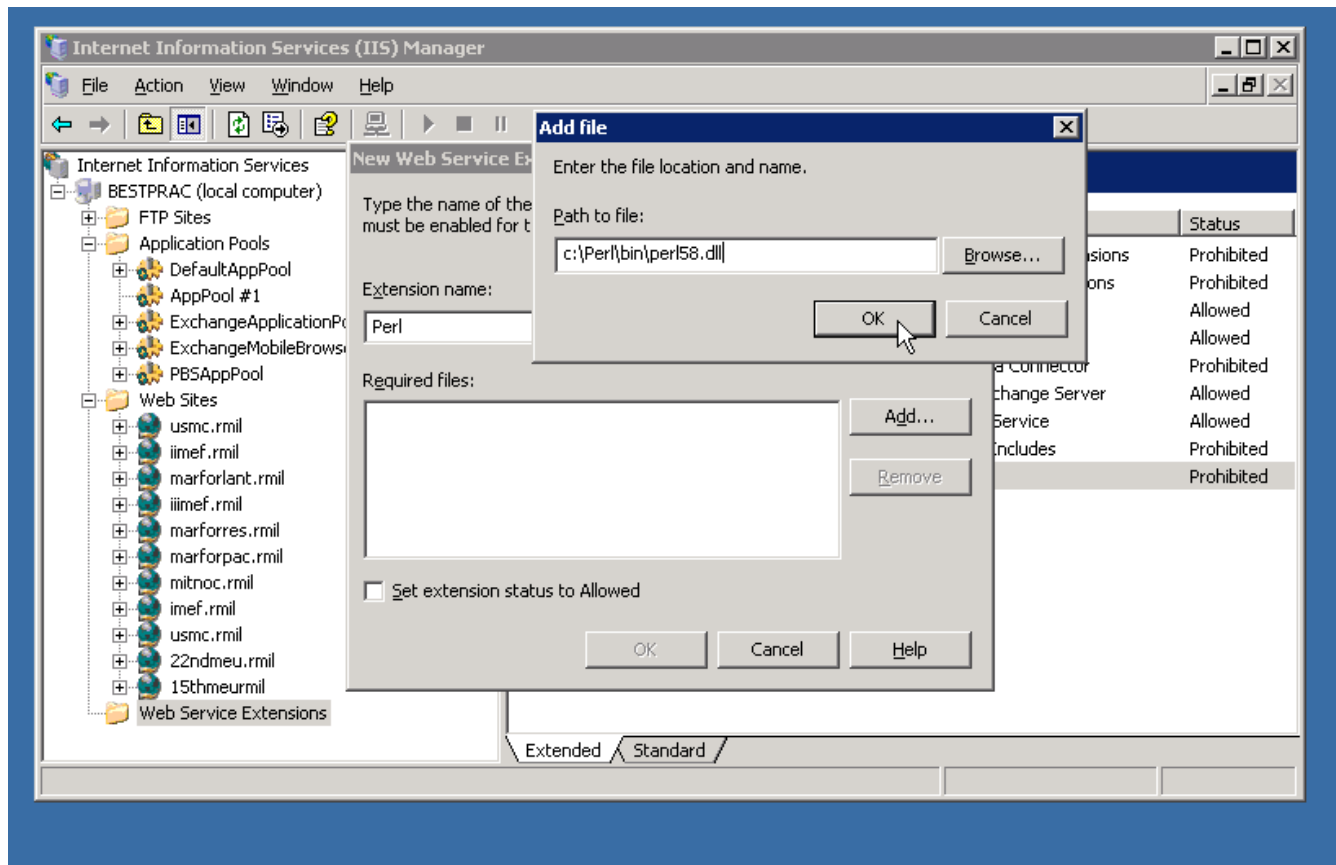
Context Menu:

- Add a new Web service extension...
- Allow all Web service extensions for a specific application...
- Prohibit all Web service extensions
- View
- New Window from Here
- Refresh
- Export List...
- Help



Adding a New Web Service Extension

MSTP





Authentication Methods

MSTP

- Two new authentication systems are available in IIS 6, however—
 - Passport Integration
 - Constrained/Delegated Authentication
- A third authentication system is available programmatically through the ASP.NET Web service extension.



Passport Integration

MSTP

- A central Web site that holds credential and user information which can then be shared among other participating sites.
- IIS 6 incorporates the capability to communicate directly with the Passport system and authenticate your users through their Passport identities
- **PASSPORT AND OTHER AUTHENTICATION TYPES:**
 - Passport cannot be used in conjunction with other authorization types because Passport operates with cookies rather than the standard HTTP-based authorization system.

Constrained, Delegated authentication



MSTP

- The two recommendations to the use of constrained, delegated authentication according to Microsoft are as follows:
 - Delegation should not enable a server to connect on behalf of the client to any resource in the domain/forest.
 - Delegation should not require the client to share its credentials with the server.

You can get more information on the steps required to enable authentication at the Microsoft Windows Server 2003 Deployment guide; the URL for the relevant page is <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/remstorg.asp>

ASP.NET Based Authentication



MSTP

- Windows authentication—provided by the standard IIS 6 authentication mechanisms and interface (that is, digest, integrated).
- Passport authentication— Works just like the integrated IIS-based Passport authentication system, but because it can be built into an ASP application, you can provide a friendlier interface.
- Forms-based authentication— Enables a developer to use a standard ASP form to request credentials that can then be authenticated through the standard mechanisms or a built-in solution.



Authorization

MSTP

- IIS 6 incorporates a new authorization framework designed to extend the object-based authorization system in previous versions.
- The new authorization framework allows developers to add and extend the authorization system based on roles, tasks, and other criteria.



SSL Improvements

MSTP

- Performance has been increased by as much as 50%
- Allow you to use third-party hardware-based accelerator cards for encrypting information over SSL.
 - SSL is a significant CPU performance hog, this can improve the speed of SSL-heavy Web sites.
- Remote Administration of certificates is now supported by enabling remote support in the cryptographic API (CAPI) certificate store.
 - Eases of administration, when managing many hundreds or thousands of sites,
- Two new wizards to help in configuring and managing the certificates
 - The Web Server Certificate Wizard
 - The Certificate Trust List Wizard.

Web Server Certificate Wizard



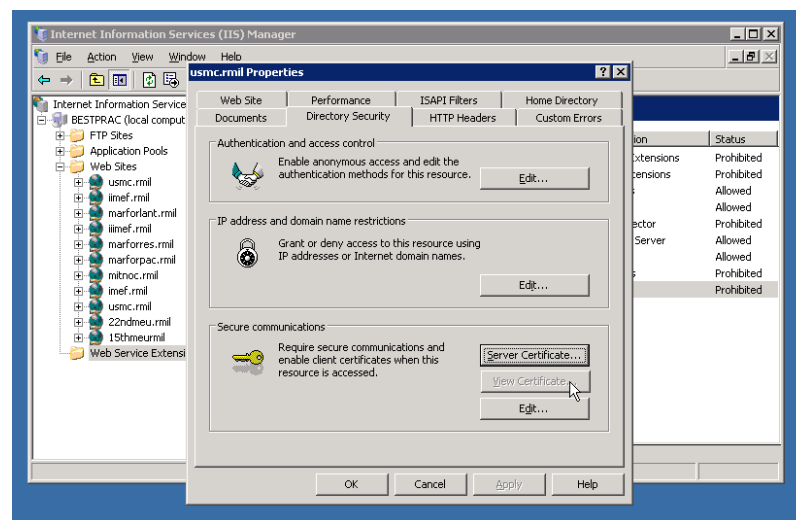
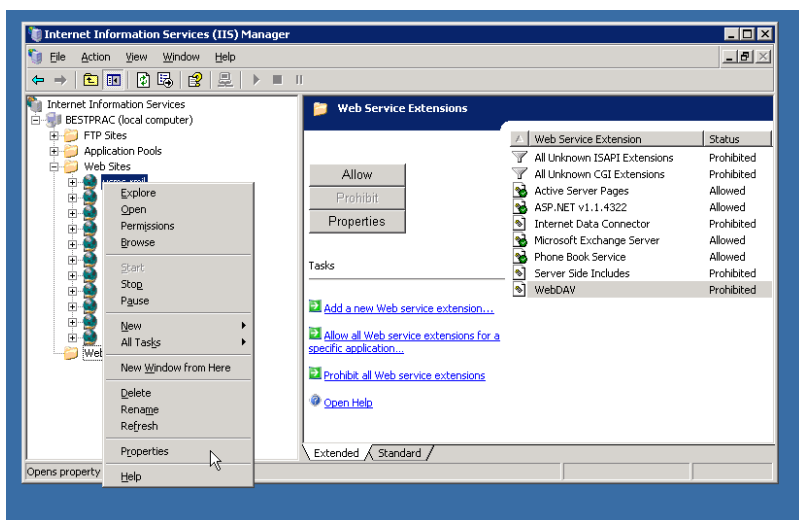
MSTP

- The Web Server Certificate Wizard is used to obtain, configure, and renew server certificates.
 - capable of creating a certificate request, replacing a server certificate.

Creating a new certificate with the IIS Certificate Wizard.



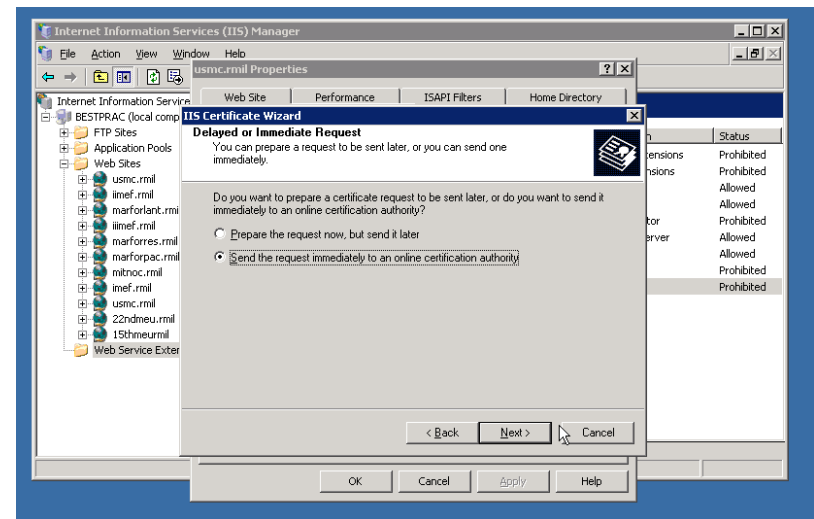
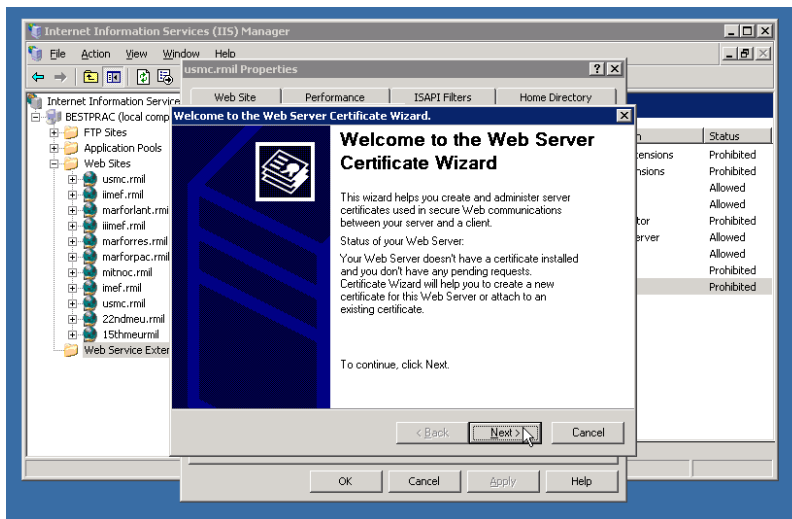
MSTP



Certificates



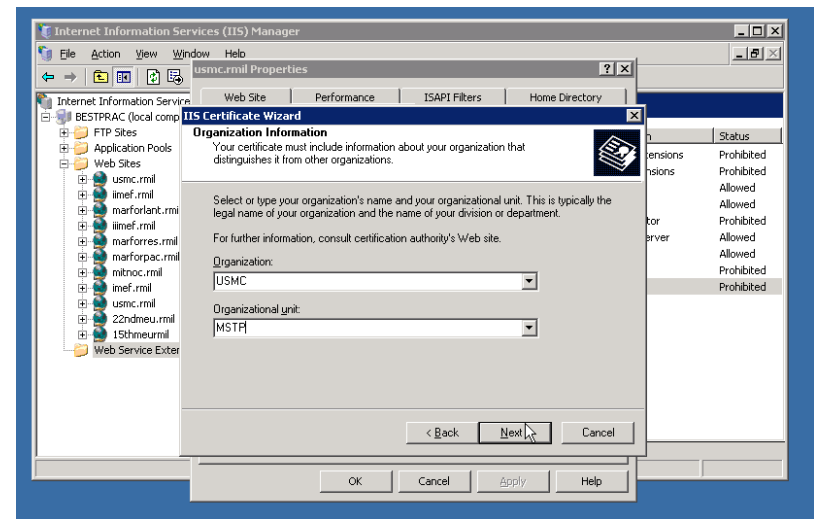
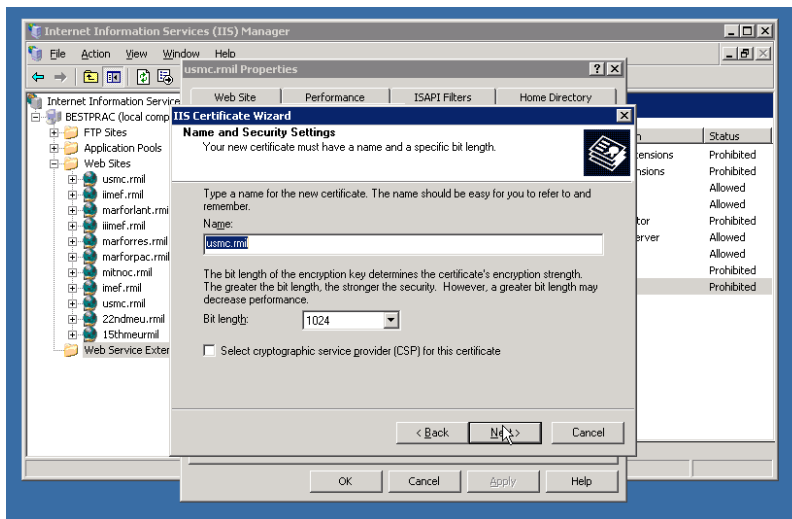
MSTP



Certificates



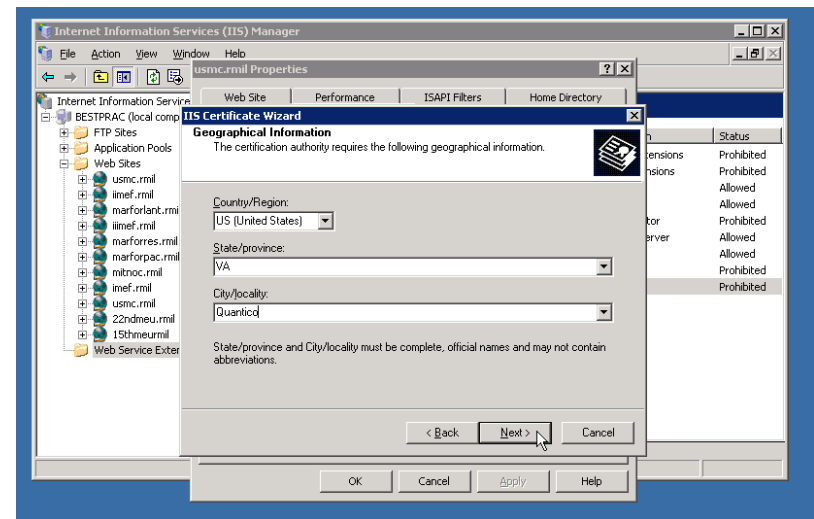
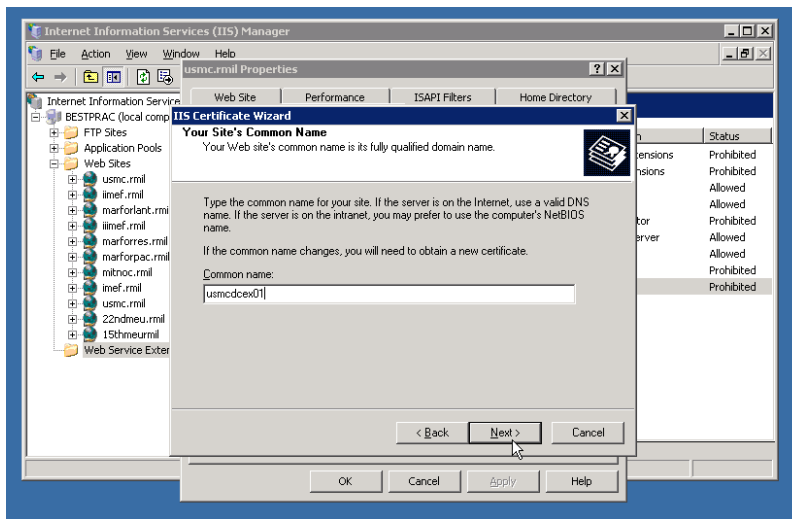
MSTP



Certificates



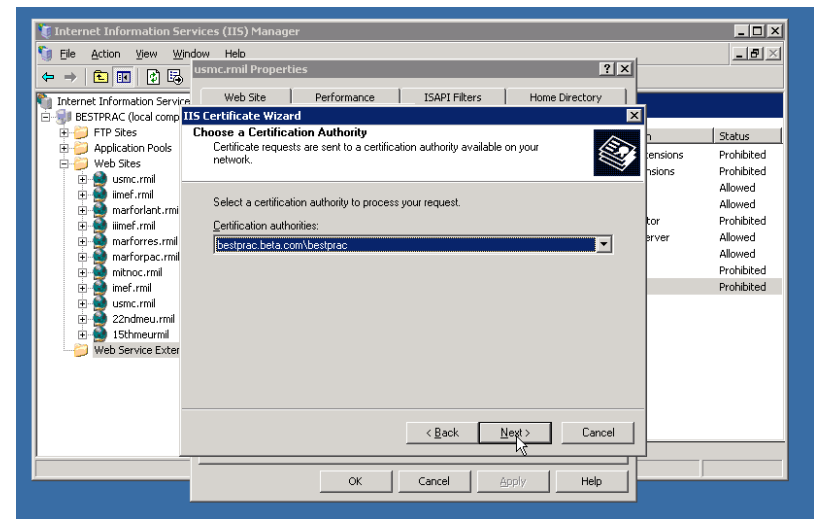
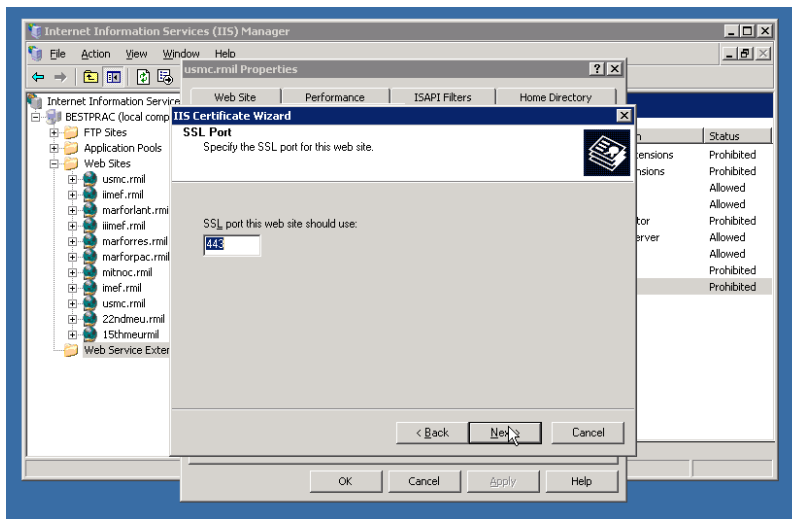
MSTP



Certificates

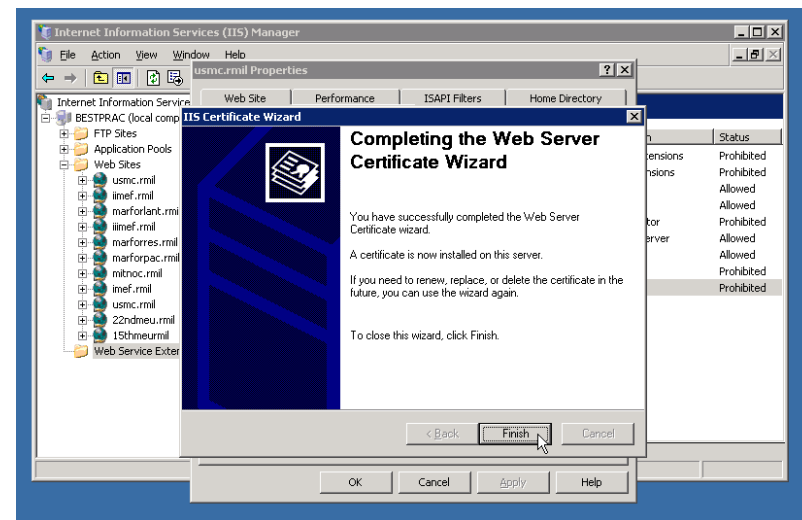
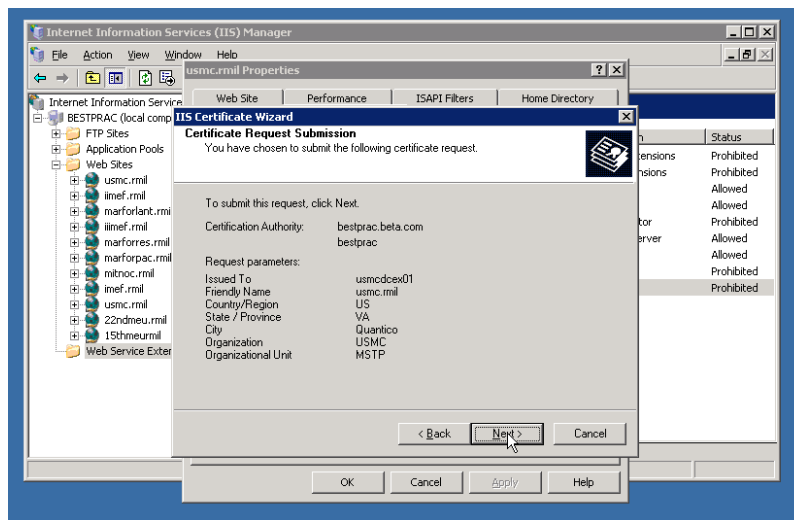


MSTP



Entering basic site information when creating a certificate request.

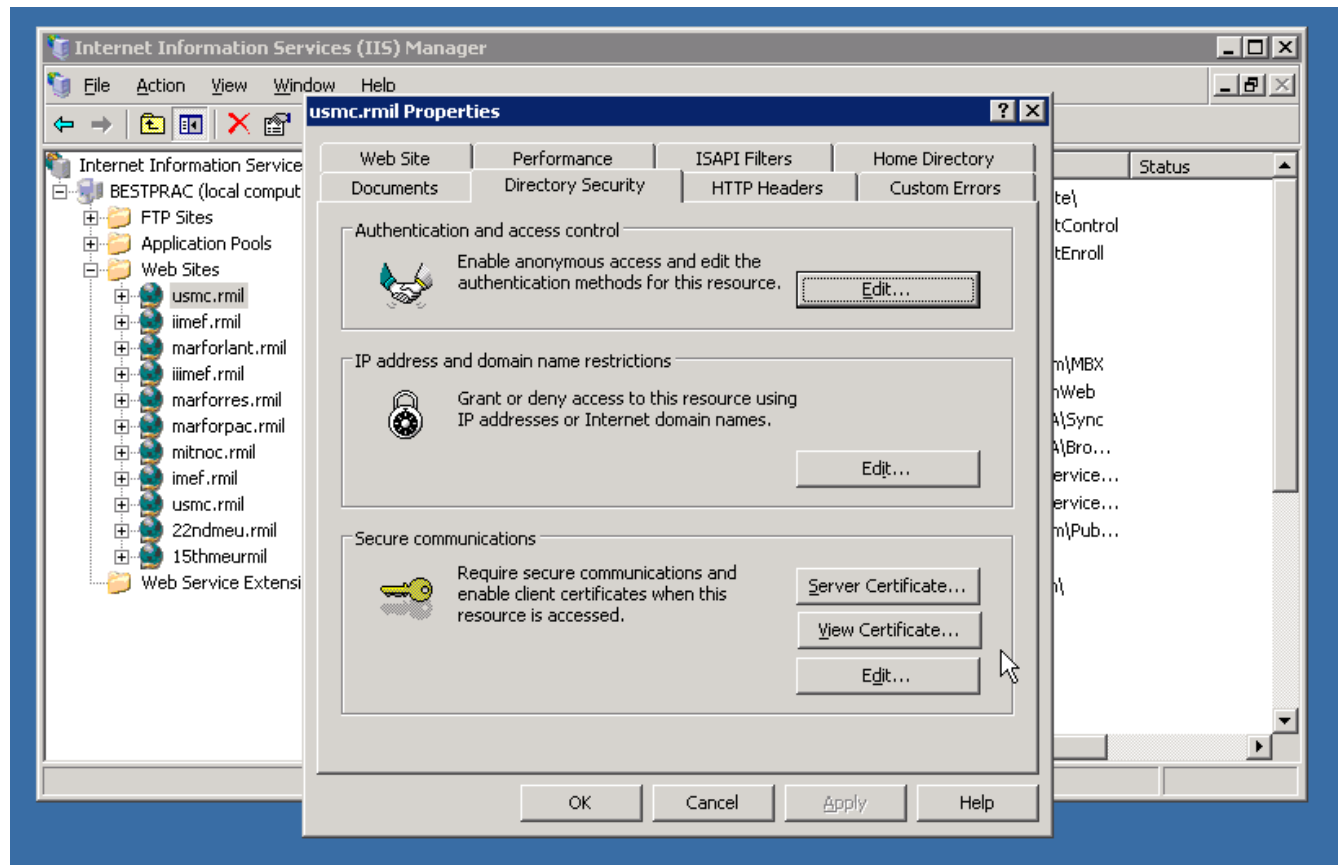
MSTP



The Certificate Property Tab



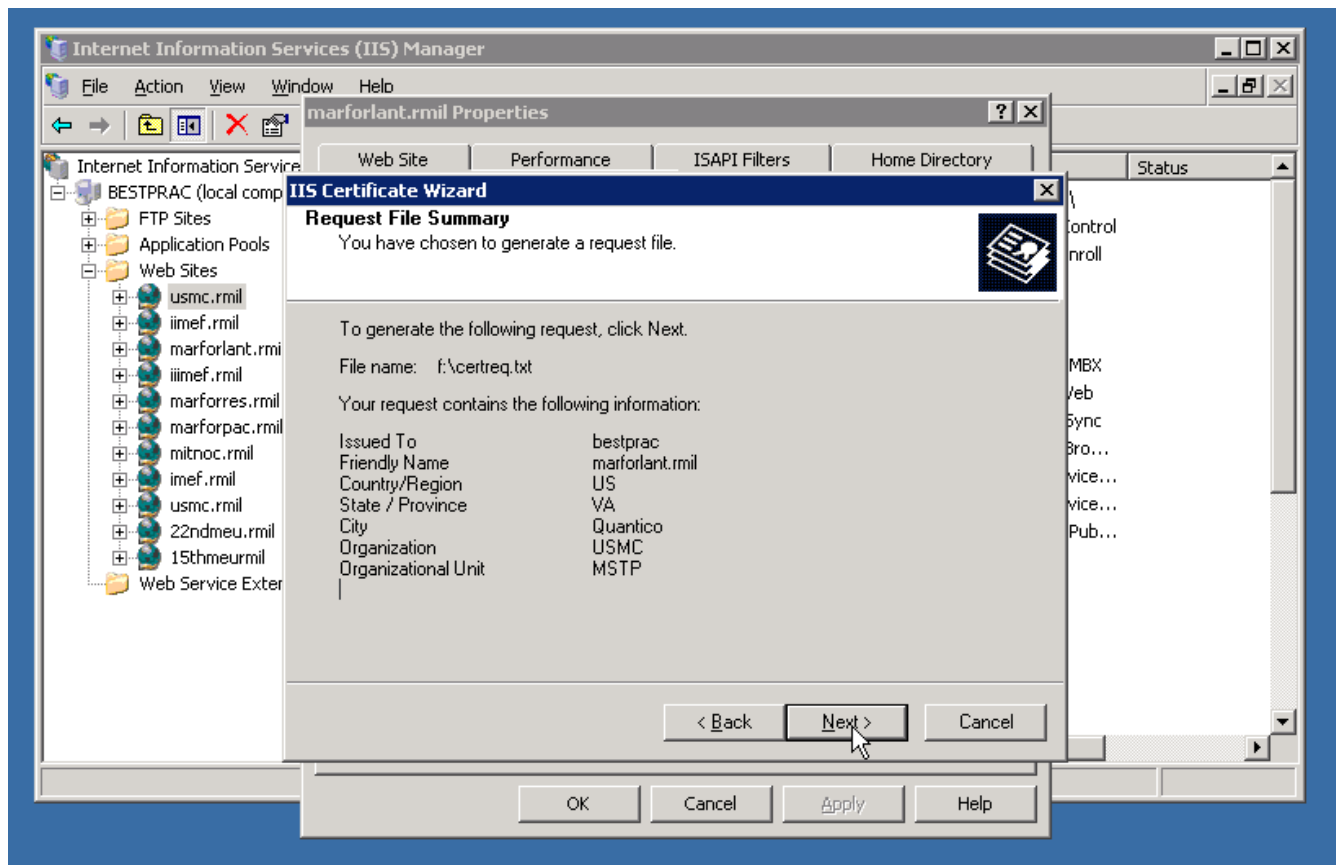
MSTP



The Certificate Property Tab



MSTP





Certificate Trust List Wizard

MSTP

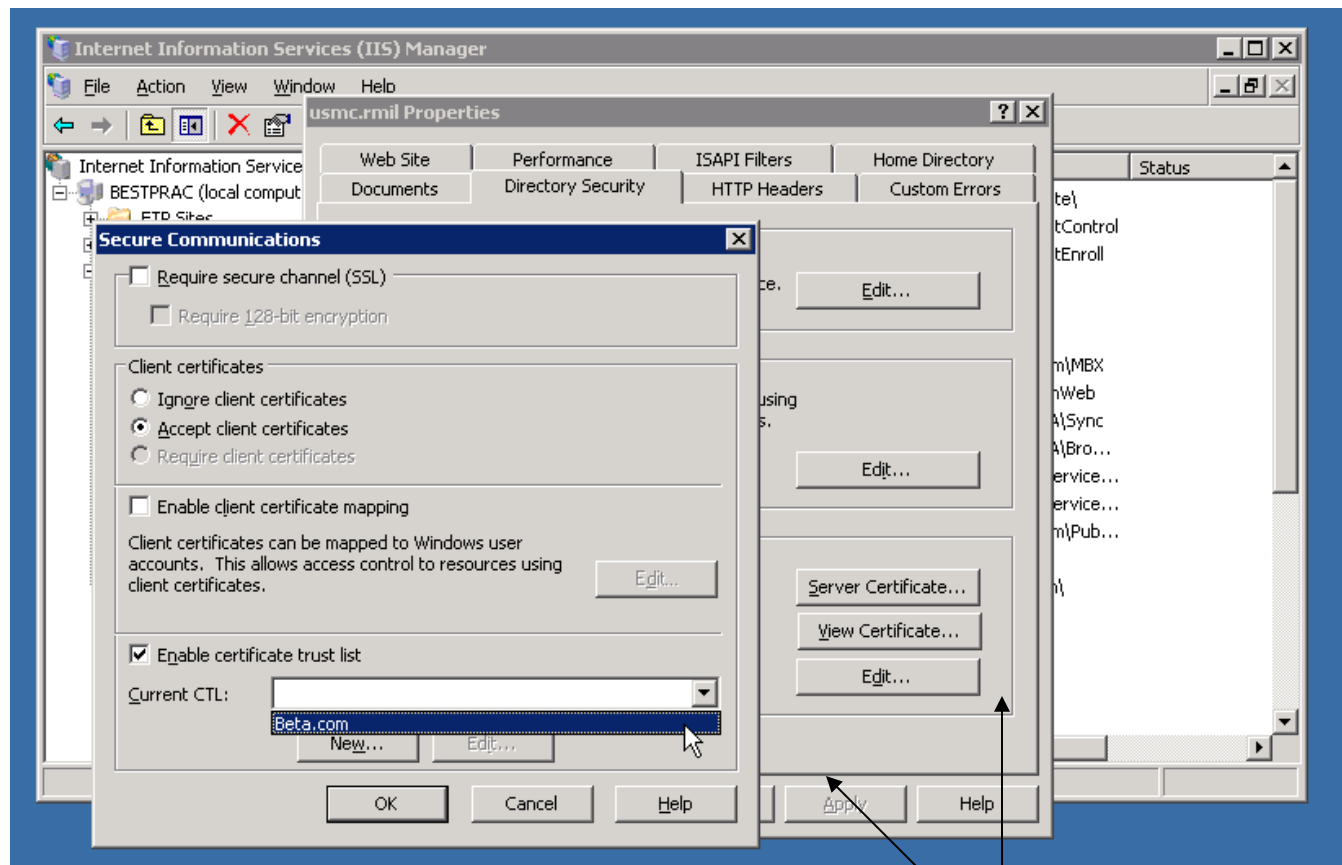
Microsoft recommends the following guidelines when assigning IP addresses, Web sites, and SSL ports to your server certificates:

- You cannot assign multiple server certificates per Web site.
- You can assign a certificate to multiple Web sites.
- You can assign multiple IP addresses per Web site.
- You can assign multiple SSL ports per Web site.

Setting secure communication options



MSTP





Worker Process Identification

MSTP

IIS 6 has updated and extended the available options:

- **ASPNET**— A local user account specifically designed to be used with the ASP.NET worker process (aspnet_wp.exe) application only when the server is running in IIS 5 isolation mode.
- **Local System**— Default user configured for all IIS and Indexing Service users.
- **Local Service**— A limited privilege account granting access to the local system only.
- **Network Service**— Provides a higher level service than that provided by the Local Service
 - ability to log on as a server and to communicate with other servers.
 - This is the default account for worker processes in worker process isolation mode.
- **IUSR_ComputerName**— The guest account used by anonymous users accessing an Internet Web site.
 - If disabled, anonymous access to the site is disabled.
- **IWAM_ComputerName**— The guest account used with Web applications.
 - If disabled, this account blocks out of process applications when operating in IIS 5 Isolation mode.
- The **IIS_WPG group** is granted the minimum rights required to start a worker process.

Default User Rights for Special IIS Users



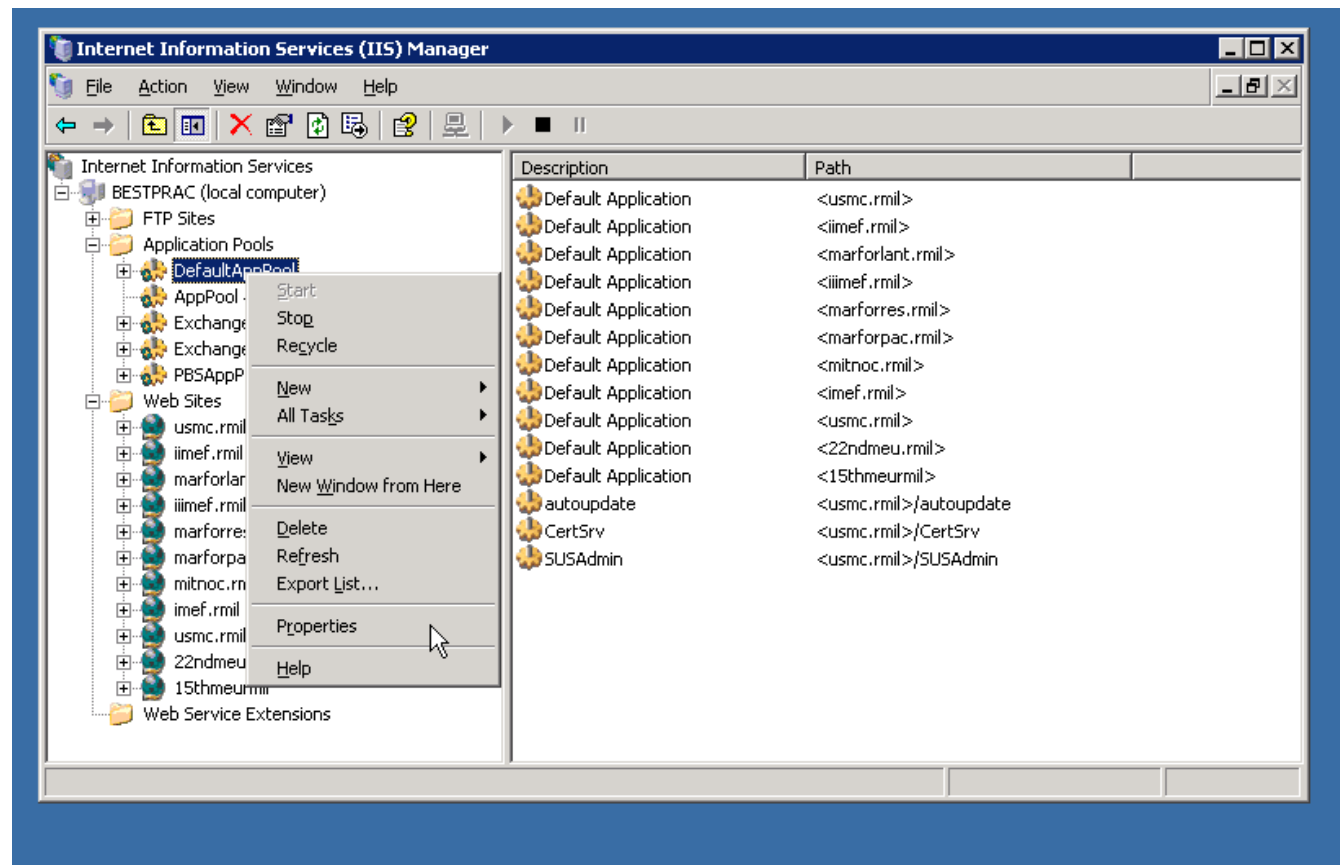
MSTP

User Right	ASPNET	Local Service	Network System	IUSR	IWAM	IIS_WPG
Access computer from the network	X	X	X	X	X	X
Adjust memory quota for a process		X	X		X	
Allow log on locally				X		
Bypass traverse checking		X	X	X	X	
Generate Security Audit		X	X			
Impersonate a client after authentication	X					X
Log on as a batch job	X	X		X	X	X
Log on as a service	X		X			
Deny Log on through terminal services	X					
Replace a process-level token		X	X		X	
Deny log on locally	X					

Setting Identity in Worker Process Isolation Mode



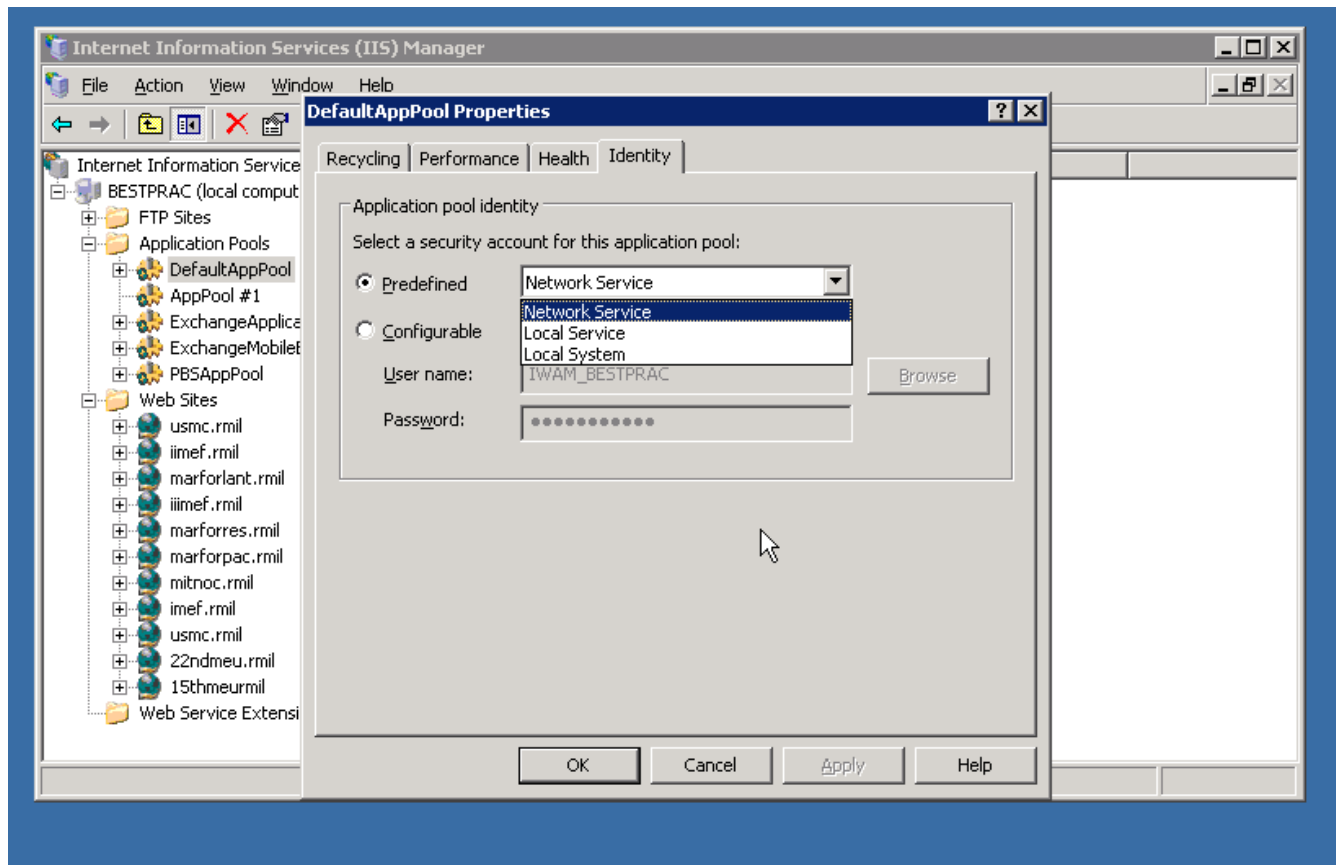
MSTP



Setting Identity in Worker Process Isolation Mode



MSTP





Setting Identity in IIS 5 Isolation Mode

MSTP

IIS Out-Of-Process Pooled Applications Properties [?] [X]

Advanced | Dump | Pooling & Recycling
General | Security | **Identity** | Activation | Queuing

This application will run under the following account.

Account

☒ System Account:


- ☐ Interactive user - The current logged on user
- ☐ Local Service - Built-in service account.
- ☐ Network Service - Built-in service account with network access
- ☐ Local System - Complete access to local machine

☒ This user:

User:

Password:

Confirm password:

 Server applications cannot run under system service accounts.



Controlling IIS Through Group Policy

MSTP

- Prevent users from installing IIS, or applications that required IIS, on Windows Server 2003 machines.
- Control IIS installations at the departmental or location/branch office level.
- You can protect other servers within your network on which you don't want IIS enabled
 - For example, a file or database server.
- The policy is within Computer Configuration, Administrative Templates, Windows Components, Internet Information Services, Prevent IIS installation.

There are only three settings:

- Enabled— Installation is prevented.
- Disabled— Machines within the domain tree are specifically allowed to install IIS.
- Not Configured— The usual propagation rules apply.

Command Line Tool Access



MSTP

- Previous versions of IIS allowed command-line tools to be executed by Web applications.
- In IIS 6, it's impossible, even as an Administrator, to execute command-line tools.
 - prevents some viruses and worms from running and propagating.



Timeouts and Limits

MSTP

- For example, when running a denial of service attack, the excessively long timeouts make it easy to saturate the server with a relatively small number of clients.
- The new worker process model helps alleviate this slightly by building in protection in the form of renewable processes for servicing user requests.



Updates and Patches

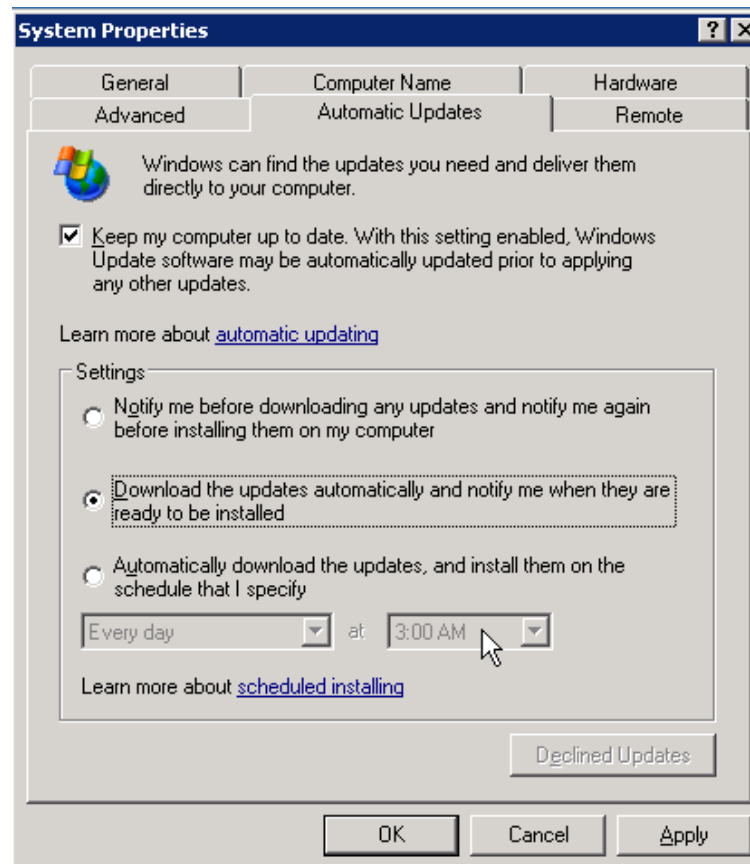
MSTP

- you should keep up-to-date with the various patches and fixes that Microsoft makes available.

Setting update intervals and

automatic installation preferences.

MSTP





FTP Security

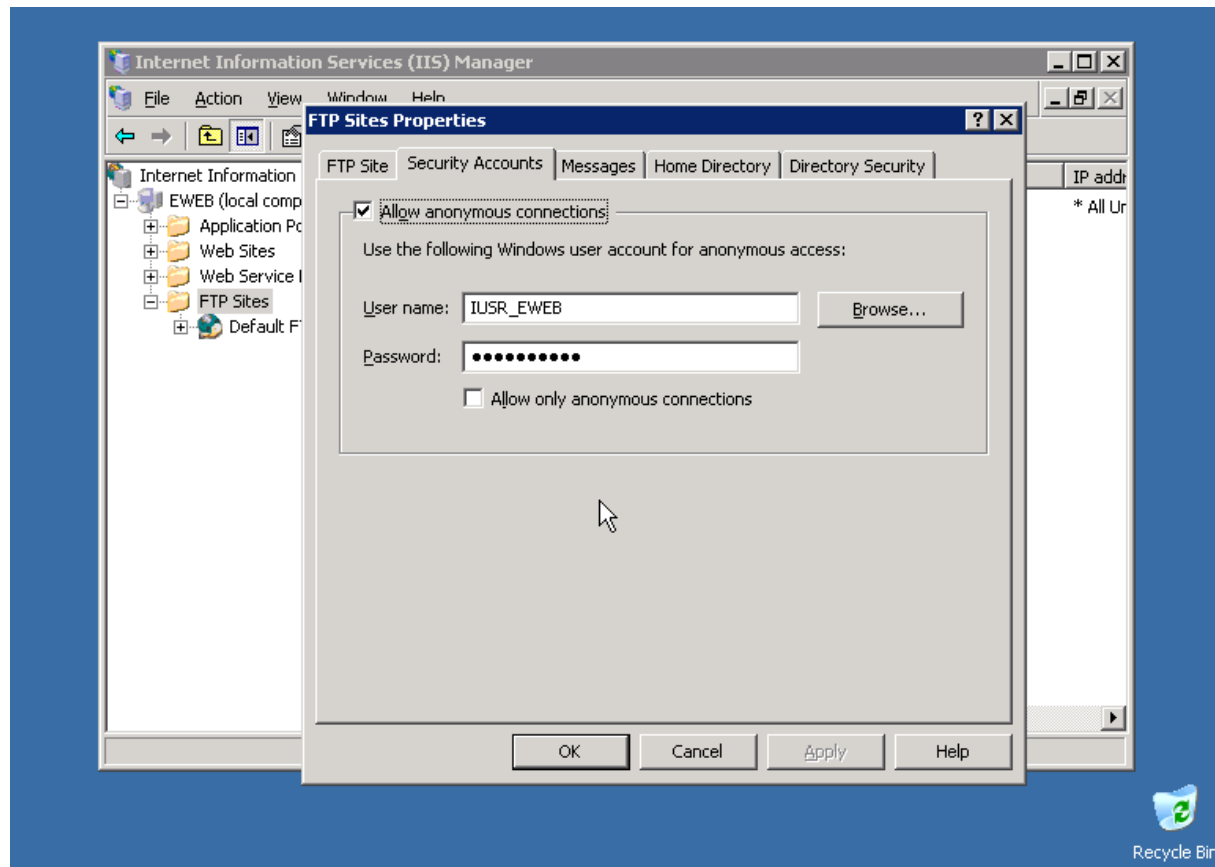
MSTP

- IIS 6, on the other hand, includes the capability to isolate users from each other—when an authorized user logs in, he can be placed in his own directory that is separate and secure from other users and the anonymous user directory.
- Three modes are available—
 - Non-isolated mode,
 - Isolated Mode,
 - Isolated Mode using Active Directory.
- You cannot switch between the different modes at will.



Granting access rights for FTP users

MSTP





Setting PASV Port Ranges

MSTP

- Passive FTP mode uses a different port number for sending files back to the client than the default FTP port of 21, which is used to send commands and responses.
- You can't configure IIS to switch off passive FTP port support, but in IIS 6 you can configure the port range used, which makes it easier to select a port range and configure your firewall service to pass through the passive FTP traffic.



Development and Deployment

MSTP

- What's New
 - The .NET system is compatible with a wide array of languages and has a rich class framework for easier development
 - Faster execution— ASP.NET applications are compiled, and their compiled forms are stored, both in memory and on disk, eliminating the need to recompile the ASP code each time it is accessed if it has already left the cache.
 - Memory, deadlock, and crash protection— Through the worker process system, it's much easier to control and recover from problems when executing an ASP component.



Development and Deployment

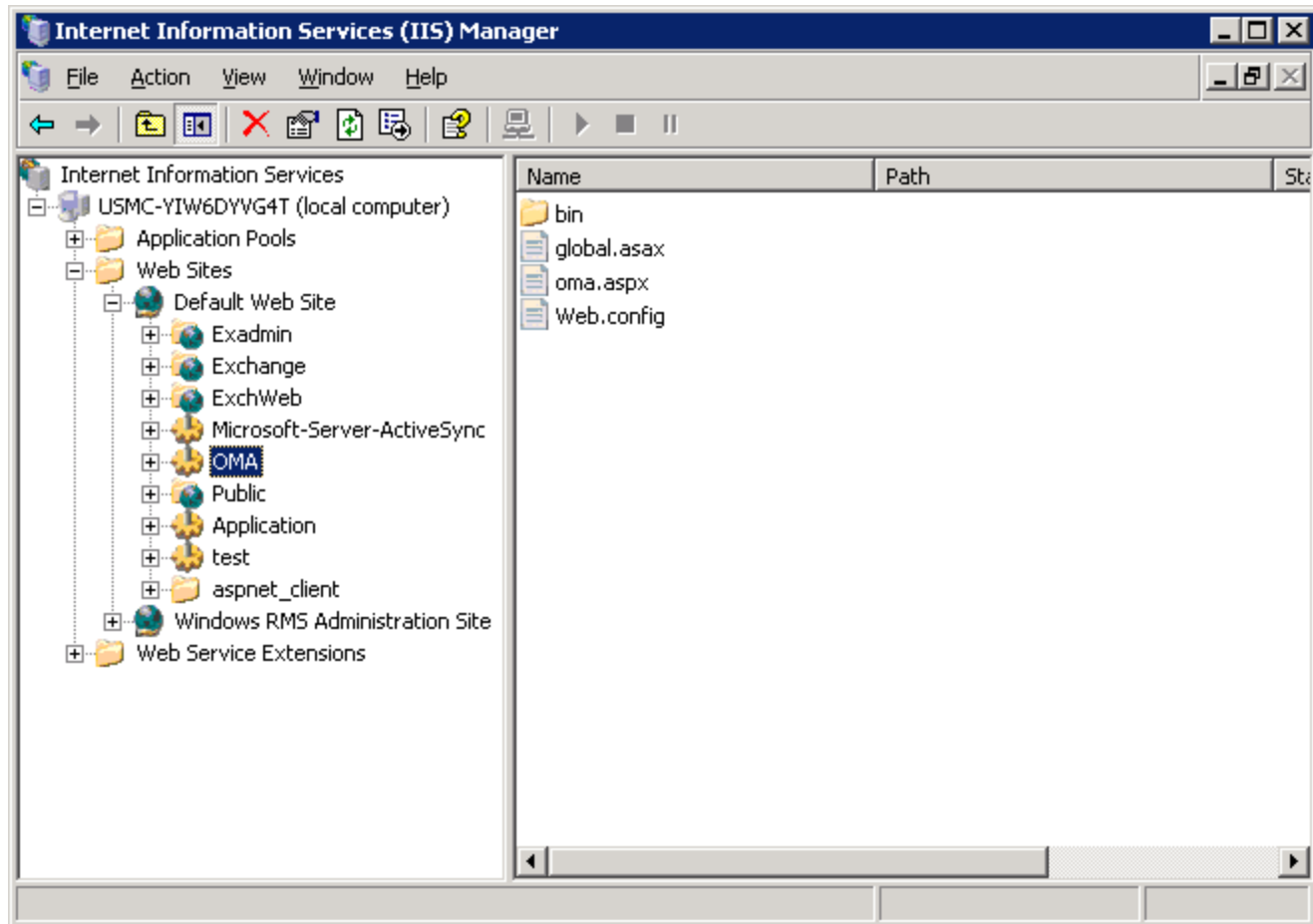
MSTP

- ISAPI Extensions
 - IIS 6 has also improved certain elements of the underlying scripting and IIS integration.
- Request Redirection (ExecuteURL)
 - Redirection is commonly used to redirect a user to an alternative page when a page has moved.
- Wildcard Application Maps
 - the extension of a file in a request is used by IIS to determine which CGI application or ISAPI filter is used to process it.



Application Configurations

MSTP





Application Configurations

MSTP

The screenshot displays two overlapping windows from the Internet Information Services (IIS) Manager. The 'OMA Properties' window is in the background, and the 'Application Configuration' window is in the foreground.

OMA Properties

- Virtual Directory** tab is selected.
- Content source: ☒ A directory located on this computer.
- Local path: Browse...
- Permissions: ☐ Script source access, ☒ Read, ☐ Write, ☐ Directory browsing.
- Log settings: ☒ Log visits, ☒ Index this resource.
- Application settings:
 - Application name: Remove
 - Starting point:
 - Execute permissions:
 - Application pool: Unload

Application Configuration

- Mappings** tab is selected.
- ☐ Cache ISAPI extensions.
- Application extensions** table:

Extens...	Executable Path	Verbs
.asa	C:\WINDOWS\system32\inetrv\asp.dll	GET,HEA..
.asax	C:\WINDOWS\Microsoft.NET\Framew...	GET,HEA..
.ascx	C:\WINDOWS\Microsoft.NET\Framew...	GET,HEA..
.ashx	C:\WINDOWS\Microsoft.NET\Framew...	GET,HEA..
.asmx	C:\WINDOWS\Microsoft.NET\Framew...	GET,HEA..

Buttons: Add..., Edit..., Remove

Wildcard application maps (order of implementation):

Buttons: Insert..., Edit..., Remove, Move Up, Move Down

Buttons: OK, Cancel, Help



Application Configurations

MSTP

- Output Caching
 - With IIS 6, two new features, VectorSend and FinalSend, simplify the process.
- Custom Errors
 - Through the ExecuteURL system, it's now possible to pass off errors within your applications to the main error handling system within IIS 6.
- Worker Process Restarting
 - A new ISAPI extension, HSE_REQ_REPORT_UNHEALTHY, can be used by an extension to force the ISAPI application's worker process to be recycled.
- COM+ Access
 - In IIS 6, COM+ can now be used independently of the COM components, allowing developers to access COM+ services directly.



Application Configurations

MSTP

- In addition, the following services have been added since Windows 2000:
- Fusion support— Enables ASP applications to use a specific version of a DLL or COM component. This is useful for backward compatibility with existing applications.
- Partition Support— COM+ partitions can now be assigned a different configuration for different users, instead of a single configuration for a specific application.
- Tracker support— Tracks when code is running within an ASP session; useful for debugging applications.



Development Platforms

MSTP

- Just as important as the built-in support within the ISAPI and deployment environments are the languages compatible with the IIS 6 platform.
 - You have two choices within IIS 6 (and in previous versions)—those available through the ASP/ASP.NET system and those available separately through the CGI and ISAPI filter systems.
- The .NET Framework is probably the biggest change in terms of deployment with IIS 6.
- Through .NET
 - .NET Framework is really a combination of a number of different technologies all designed to work together to provide better cooperation, integration, and faster development times.
 - more than 25 languages were certified compatible with .NET



Independent Options

MSTP

- Perl— This is available in both CGI and ISAPI compatible alternatives through the ActivePerl distribution from ActiveState.
- Python— Also available from ActiveState (as ActivePython) for use with IIS.
- PHP— Available in an ISAPI compatible state from php.net.

Web Services



MSTP

- Web Services are an architecture and platform neutral method of providing access to services and of exchanging information between clients and servers, as well as between servers while executing a request.
- **Unicode Support**
 - One of the many problems faced by IIS managers and Web developers is the issue of languages and providing multiple language Web sites for users.
 - Unicode support is built into IIS 6 in terms of supporting static files



Troubleshooting

MSTP

What problem are you having?

- I received the "Cannot find server" error message.
 - **Cause:** Your server is not available.
 - **Solution:** To determine why the server is unavailable, ping your IIS server and try to determine the problem based on the results of the ping. Use the ping command at the command line. Before you can ping your server, you need to determine the server name or its IP address. If you want to ping your server by name and your server is on an intranet, you need to know its NetBIOS name. If you want to ping your server by name and your server connects to the Internet, you need to know its fully qualified domain name (FQDN).
- To ping the server by using the NetBIOS name
- To ping the server by using the FQD
- To ping the server by using the IP address



Troubleshooting

MSTP

- I received the "The page cannot be displayed" error message.
 - **Cause:** IIS is not responding.
 - **Solution:** Restart IIS.
- **To restart a Web site / WWW Service**
 1. Click **Start**, and then click **Run**.
 2. In **Open**, type **inetmgr**, and then click **OK**.
 3. Open the server node in the console tree. An asterisk between the server icon and the server name indicates the local server.
 4. Click the Web site that you want to restart.
 5. From the **Action** menu, click **Stop**. When the site is stopped, **(Stopped)** appears next to the site name in the console tree.
 6. To restart the Web site, from the Action menu, click **Start**.

Troubleshooting



MSTP

- I received the "Under Construction" error message or "The site you are trying to reach does not currently have a default page" error message.
 - **Cause:** IIS is unable to locate the default page for your Web site.
 - **Solution:** Verify or change the location of your default Web site. By default, the files for your default Web site are located at `X:\inetpub\wwwroot`, where `X` is the drive on which your Windows Server 2003 operating system is installed. For example, if Windows Server 2003, Standard Edition, is installed to your `C:` drive, the content files for your default home page are stored at `C:\inetpub\wwwroot`. You need to test the location of your content files from the server that is running IIS.



Troubleshooting

MSTP

- You are unable to serve dynamic content and IIS has returned a 404 error.
 - **Cause:** When you install IIS, the service is installed in a highly secure and locked mode. By default, IIS serves only static content, which means that features such as Active Server Pages (ASP), ASP.NET, Indexing Service, server-side includes (SSI), Web Distributed Authoring and Versioning (WebDAV), and FrontPage Server Extensions do not work unless you enable them. If you do not enable these features after installing IIS, IIS returns a 404 error.
 - **Solution:** To serve dynamic content and unlock these features, you must enable them by using IIS Manager. Administrators can enable or disable IIS functionality based on the needs of the organization. Also, if an application extension is not mapped in IIS, IIS returns a 404 error. To map an application extension, see "Setting Application Mappings" in IIS 6.0 Help. For more information about troubleshooting 404 errors, see "Troubleshooting" in IIS 6.0 Help. For information about how to open IIS 6.0 Help, see To view Internet Information Services (IIS) 6.0 Help .